

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-306332

(43)Date of publication of application : 02.11.2000

(51)Int.Cl.

G11B 20/10

(21)Application number : 2000-039265

(71)Applicant : SONY CORP

(22)Date of filing : 17.02.2000

(72)Inventor : KAWAKAMI TATSU

ISHIGURO RYUJI

TANABE MITSURU

EOMO YUICHI

(30)Priority

Priority number : 11039221

Priority date : 17.02.1999

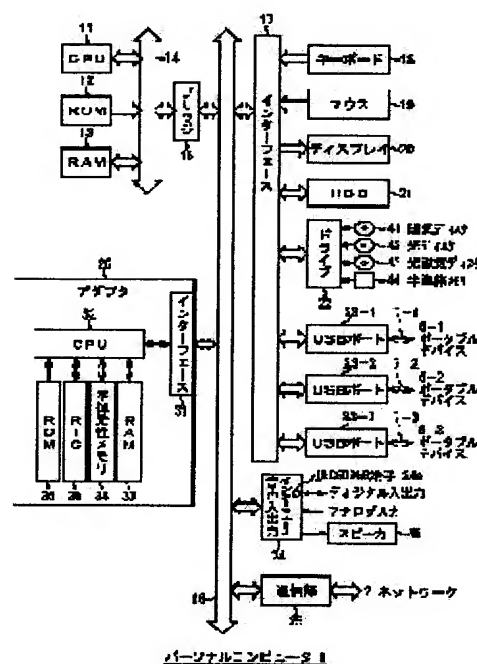
Priority country : JP

(54) APPARATUS AND METHOD FOR PROCESSING INFORMATION, AND PROGRAM
STORING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To make effectively preventable an illegal copy of data received from other apparatus.

SOLUTION: For recording on an HDD 21 musical data transferred from an EMD server via internet, a CPU 11 executes a mutual authentication processing with the EMD server, using a fixed key stored in a nonvolatile memory 34 and has a communicating key in common. The EMD server encrypts music data with the communicating key and transfers it to a personal computer 1. The CPU 11 records the transferred encrypted data on the HDD 21, encrypts the communicating key with a reserved key stored in the memory 34 and records it on the HDD 21.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-306332
(P2000-306332A)

(43) 公開日 平成12年11月2日 (2000. 11. 2)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H
			F

審査請求 未請求 請求項の数 4 O L (全 38 頁)

(21) 出願番号 特願2000-39265 (P2000-39265)
(22) 出願日 平成12年2月17日 (2000. 2. 17)
(31) 優先権主張番号 特願平11-39221
(32) 優先日 平成11年2月17日 (1999. 2. 17)
(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号
(72) 発明者 河上 達
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(72) 発明者 石黒 隆二
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内
(74) 代理人 100082131
弁理士 稲本 義雄

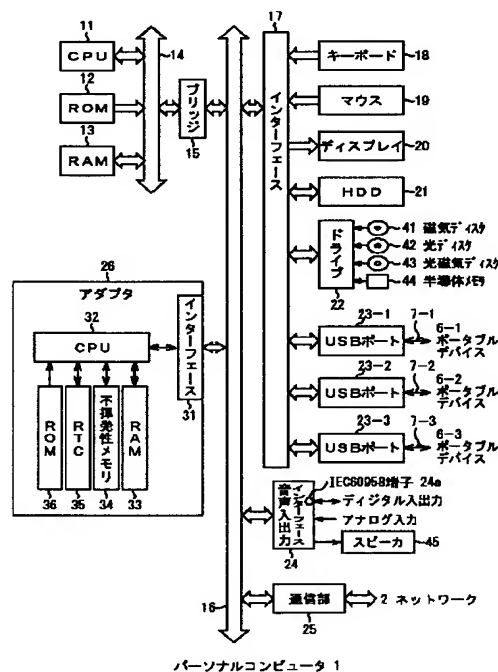
最終頁に続く

(54) 【発明の名称】 情報処理装置および方法、並びにプログラム格納媒体

(57) 【要約】

【課題】 他の装置から受信したデータが不正に複製されるのを効果的に防止する。

【解決手段】 CPU 11 は、EMDサーバからインターネットを介して転送されてきた音楽データをHDD 21に記録するとき、不揮発性メモリ 34に記憶されている固定鍵を用いて、EMDサーバと相互認証処理を行い、通信用鍵を共有する。EMDサーバは、通信用鍵で暗号化して音楽データをパーソナルコンピュータ 1に転送する。CPU 11は、転送を受けた暗号化されている音楽データをHDD 21に記録するとともに、通信用鍵を不揮発性メモリ 34に記憶されている保存用鍵で暗号化して、HDD 21に記録する。



【特許請求の範囲】

【請求項 1】 他の装置との間でデータを授受する授受手段と、

所定の固定鍵と保存用鍵を保持する保持手段と、
前記他の装置との間でデータを授受するとき、前記保持手段に保持されている前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証手段と、

前記通信用鍵を、前記保存用鍵で暗号化する暗号化手段と、

前記授受手段により受信された、前記通信用鍵で暗号化されているデータを、前記暗号化手段により暗号化された前記通信用鍵と対応させて蓄積する蓄積手段とを含むことを特徴とする情報処理装置。

【請求項 2】 前記蓄積手段に蓄積されている前記通信用鍵を、前記保存用鍵を用いて復号する暗号鍵復号手段と、

前記暗号鍵復号手段により復号された前記通信用鍵を用いて、前記蓄積手段に蓄積されているデータを復号するデータ復号手段とをさらに含むことを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 他の装置との間でデータを授受する授受ステップと、

所定の固定鍵と保存用鍵を保持する保持ステップと、
前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、

前記通信用鍵を、前記保存用鍵で暗号化する暗号化ステップと、

前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含むことを特徴とする情報処理方法。

【請求項 4】 他の装置との間でデータを授受する授受ステップと、

所定の固定鍵と保存用鍵を保持する保持ステップと、
前記他の装置との間でデータを授受するとき、前記保持ステップの処理で保持された前記固定鍵を利用して、前記他の装置と相互認証処理を行い、通信用鍵を生成する認証ステップと、

前記通信用鍵を、前記保存用鍵で暗号化する暗号化ステップと、

前記授受ステップの処理で受信された、前記通信用鍵で暗号化されているデータを、前記暗号化ステップの処理で暗号化された前記通信用鍵と対応させて蓄積する蓄積ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが格納されているプログラム格納媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、並びにプログラム格納媒体に関し、特に、通信路の途中でデータ漏洩し、複製されるのを防止することができるようにした、情報処理装置および方法、並びにプログラム格納媒体に関する。

【0002】

【従来の技術】最近、デジタル技術の普及にともない、音楽データ、画像データなどの各種のデータがデジタル的に記録媒体に記録または再生されるようになってきた。その結果、複数回コピーしても、画質あるいは音質が劣化しないデータを得ることが可能となってきた。

【0003】

【発明が解決しようとする課題】しかしながら、このようにデジタル技術が発達してくると、次のような問題が発生する。

【0004】(1) 例えば、コンパクトディスク (CD) からパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、CDからの音楽データが、そのまま、あるいは圧縮符号化されてハードディスクに記録されるので、例えば、インターネットなどのネットワークを介して複製を違法に大量に配布することができてしまう。

【0005】(2) CDからパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、そのコピーの回数に制限がないため、複製が大量に配布されてしまう。

【0006】(3) パーソナルコンピュータのハードディスク内のデジタル音楽データを、例えば、ポータブルデバイスなどの外部の機器に移す場合、移した後もハードディスク内に元のデジタル音楽データが残るので、複製が大量に配布できてしまう恐れがある。

【0007】(4) 上記した(3)の問題を防止するために、デジタル音楽データを外部の機器に移した後に、データの送り元としてのハードディスクのデータを消去するように (いわゆる、音楽データをムーブするように) パーソナルコンピュータのソフトウェアを作成しておけばよいが、例えば、ムーブの前にハードディスクの内容を別の記録媒体へバックアップしておき、ムーブの後に、バックアップしたデータをハードディスクにリストアすれば、結局、ムーブしたはずのデータがハードディスクに残ってしまうことになる。

【0008】(5) パーソナルコンピュータが、ハードディスク内のデジタル音楽データをポータブルデバイスなどの外部の機器に移す場合、外部機器がどのような機器であるかを確認しないため、違法な機器にデジタル音楽データが渡されてしまう恐れがある。

【0009】(6) ポータブルデバイスなどの外部の機器から、パーソナルコンピュータにデジタル音楽データを渡す場合、そのパーソナルコンピュータを制御して

10

20

30

40

50

いるソフトウェアがどのようなソフトウェアであるかを
確認しないため、違法なソフトウェアに対してデジタル
音楽データが渡されてしまう恐れがある。

【0010】(7) CDより再生された音楽データをパ
ーソナルコンピュータで取り扱うとき、複数の曲が同一
か否かを判断するために、曲データに含まれるISRC (In
ternational Standard Recording Code) を使用すること
が可能であるが、CDによっては、ISRCデータを含んで
いないものがある。この場合、複数の曲が同一であるか
否かを判定することができなくなる。

【0011】(8) 以上のような各機能は、パーソナ
ルコンピュータ上で、ソフトウェアの制御により実現さ
れるため、そのソフトウェアが改竄されると、システム
の作成者が意図しない動作を行わせることができてしま
う。

【0012】本発明はこのような状況に鑑みてなされた
ものであり、ハードディスク内のデジタル音楽データを
外部の機器に渡す場合に、音楽データが漏洩し、不正に
複製されるのを防止するようにするものである。

【0013】

【課題を解決するための手段】請求項1に記載の情報処
理装置は、他の装置との間でデータを授受する授受手段
と、所定の固定鍵と保存用鍵を保持する保持手段と、他
の装置との間でデータを授受するとき、保持手段に保持
されている固定鍵を利用して、他の装置と相互認証処理
を行い、通信用鍵を生成する認証手段と、通信用鍵を、
保存用鍵で暗号化する暗号化手段と、授受手段により受
信された、通信用鍵で暗号化されているデータを、暗号
化手段により暗号化された通信用鍵と対応させて蓄積す
る蓄積手段とを含むことを特徴とする。

【0014】情報処理装置は、蓄積手段に蓄積されてい
る通信用鍵を、保存用鍵を用いて復号する暗号鍵復号手
段と、暗号鍵復号手段により復号された通信用鍵を用い
て、蓄積手段に蓄積されているデータを復号するデータ
復号手段とをさらに設けることができる。

【0015】請求項3に記載の情報処理方法は、他の装
置との間でデータを授受する授受ステップと、所定の固
定鍵と保存用鍵を保持する保持ステップと、他の装置と
の間でデータを授受するとき、保持ステップの処理で保
持された固定鍵を利用して、他の装置と相互認証処理を
行い、通信用鍵を生成する認証ステップと、通信用鍵
を、保存用鍵で暗号化する暗号化ステップと、授受ステ
ップの処理で受信された、通信用鍵で暗号化されている
データを、暗号化ステップの処理で暗号化された通信用
鍵と対応させて蓄積する蓄積ステップとを含むことを特
徴とする。

【0016】請求項4に記載のプログラム格納媒体のプ
ログラムは、他の装置との間でデータを授受する授受ス
テップと、所定の固定鍵と保存用鍵を保持する保持ステ
ップと、他の装置との間でデータを授受するとき、保持

ステップの処理で保持された固定鍵を利用して、他の装
置と相互認証処理を行い、通信用鍵を生成する認証ステ
ップと、通信用鍵を、保存用鍵で暗号化する暗号化ステ
ップと、授受ステップの処理で受信された、通信用鍵で
暗号化されているデータを、暗号化ステップの処理で暗
号化された通信用鍵と対応させて蓄積する蓄積ステップ
とを含むことを特徴とする。

【0017】請求項1に記載の情報処理装置、請求項3
に記載の情報処理方法、および請求項4に記載のプログ
ラム格納媒体においては、他の装置との間でデータを授
受するとき保持されている固定鍵を利用して、他の装置
との間で相互認証処理が行われ、通信用鍵が生成され
る。通信用鍵は、保存用鍵で暗号化され、通信用鍵で暗
号化されているデータとともに蓄積される。

【0018】

【発明の実施の形態】図1は、本発明に係るコンテン
ツデータ管理システムの一実施の形態を示す図である。パ
ーソナルコンピュータ1は、ローカルエリアネットワー
クまたはインターネットなどから構成されるネットワー
ク2に接続されている。パーソナルコンピュータ1は、
EMD (Electrical Music Distribution) サーバ4-1乃至
4-3から受信した、または後述するCD (Compact Di
sc) から読み取った楽音のデータ (以下、コンテンツと
称する) を、所定の圧縮の方式 (例えば、ATRAC3 (商
標)) に変換するとともにDES (Data Encryption Stand
ard) などの暗号化方式で暗号化して記録する。

【0019】パーソナルコンピュータ1は、暗号化して
記録しているコンテンツに対応して、コンテンツの利用
条件を示す利用条件のデータを記録する。

【0020】利用条件のデータは、例えば、その利用条
件のデータに対応するコンテンツを同時に利用すること
ができるポータブルデバイス (Portable Device (PDと
も称する)) の台数 (後述する、いわゆるチェックア
ウトできるPDの台数) を示す。利用条件のデータに示さ
れる数だけコンテンツをチェックアウトしたときでも、パ
ーソナルコンピュータ1は、そのコンテンツを再生でき
る。

【0021】または、利用条件のデータは、コピーする
ことができることを示す。コンテンツをポータブルデバ
イス6-1乃至6-3にコピーしたとき、パーソナルコン
ピュータ1は記録しているコンテンツを再生できる。
コンテンツの、ポータブルデバイス6-1乃至6-3に
記憶させることができる回数は、制限される場合があ
る。この場合、コピーできる回数は、増えることがな
い。

【0022】または、利用条件のデータは、他のパー
ソナルコンピュータに移動することができるなどを示す。
ポータブルデバイス6-1乃至6-3にコンテンツを移
動させた後、パーソナルコンピュータ1が記録している
コンテンツは使用できなくなる (コンテンツが削除され

10

20

30

40

50

るか、または利用条件が変更されて使用できなくなる)。

【0023】利用条件のデータの詳細は、後述する。

【0024】パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータ(例えば、曲名、または再生条件など)と共に、USB(Universal Serial Bus)ケーブル7-1を介して、接続されているポータブルデバイス6-1に記憶させるとともに、ポータブルデバイス6-1に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する(以下、チェックアウトと称する)。より詳細には、チェックアウトしたとき、パーソナルコンピュータ1が記録している、そのコンテンツに対応する利用条件のデータのチェックアウトできる回数は、1減らされる。チェックアウトできる回数が0のとき、対応するコンテンツは、チェックアウトすることができない。

【0025】パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USBケーブル7-2を介して、接続されているポータブルデバイス6-2に記憶させるとともに、ポータブルデバイス6-2に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1は、暗号化して記録しているコンテンツを、コンテンツに関連するデータと共に、USBケーブル7-3を介して、接続されているポータブルデバイス6-3に記憶させるとともに、ポータブルデバイス6-3に記憶させたことに対応して、記憶させたコンテンツに対応する利用条件のデータを更新する。

【0026】また、パーソナルコンピュータ1は、USBケーブル7-1を介して、接続されているポータブルデバイス6-1にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-1に消去させて(または、使用できなくさせて)、消去させたコンテンツに対応する利用条件のデータを更新する(以下、チェックインと称する)。より詳細には、チェックインしたとき、パーソナルコンピュータ1が記録している、対応するコンテンツの利用条件のデータのチェックアウトできる回数は、1増やされる。

【0027】パーソナルコンピュータ1は、USBケーブル7-2を介して、接続されているポータブルデバイス6-2にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-2に消去させて(または、使用できなくさせて)、消去させたコンテンツに対応する利用条件のデータを更新する。パーソナルコンピュータ1は、USBケーブル7-3を介して、接続されているポータブルデバイス6-3にパーソナルコンピュータ1がチェックアウトしたコンテンツを、ポータブルデバイス6-3に消去させて(または、使用でき

なくさせて)、消去させたコンテンツに対応する利用条件のデータを更新する。

【0028】パーソナルコンピュータ1は、図示せぬ他のパーソナルコンピュータがポータブルデバイス6-1にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6-2にチェックアウトしたコンテンツをチェックインできない。パーソナルコンピュータ1は、他のパーソナルコンピュータがポータブルデバイス6-3にチェックアウトしたコンテンツをチェックインできない。

【0029】EMD登録サーバ3は、パーソナルコンピュータ1がEMDサーバ4-1乃至4-3からコンテンツの取得を開始するとき、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、パーソナルコンピュータ1とEMDサーバ4-1乃至4-3との相互認証に必要な認証鍵をパーソナルコンピュータ1に送信するとともに、EMDサーバ4-1乃至4-3に接続するためのプログラムをパーソナルコンピュータ1に送信する。

【0030】EMDサーバ4-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータ(例えば、曲名、または再生制限など)と共に、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-2は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ1にコンテンツを供給する。EMDサーバ4-3は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツに関連するデータと共に、パーソナルコンピュータ1にコンテンツを供給する。

【0031】EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一または異なる圧縮の方式で圧縮されている。EMDサーバ4-1乃至4-3のそれぞれが供給するコンテンツは、同一または異なる暗号化の方式で暗号化されている。

【0032】WWW(World Wide Web)サーバ5-1は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったCD(例えば、CDのアルバム名、またはCDの販売会社など)、およびCDから読み取ったコンテンツに対応するデータ(例えば、曲名、または作曲者名など)をパーソナルコンピュータ1に供給する。WWWサーバ5-2は、パーソナルコンピュータ1の要求に対応して、ネットワーク2を介して、コンテンツを読み取ったCD、およびCDから読み取ったコンテンツに対応するデータをパーソナルコンピュータ1に供給する。

【0033】ポータブルデバイス6-1は、パーソナルコンピュータ1から供給されたコンテンツ(すなわち、チェックアウトされたコンテンツ)を、コンテンツに関

連するデータ（例えば、曲名、または再生制限など）と共に記憶する。ポータブルデバイス6-1は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。

【0034】例えば、コンテンツに関連するデータとして記憶されている、再生制限としての再生回数を超えて再生しようとしたとき、ポータブルデバイス6-1は、対応するコンテンツの再生を停止する。コンテンツに関連するデータとして記憶されている再生制限としての、再生期限を過ぎた後に再生しようとしたとき、ポータブルデバイス6-1は、対応するコンテンツの再生を停止する。

【0035】使用者は、コンテンツを記憶したポータブルデバイス6-1をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0036】ポータブルデバイス6-2は、パーソナルコンピュータ1から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス6-2は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス6-2をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0037】ポータブルデバイス6-3は、パーソナルコンピュータ1から供給されたコンテンツを、コンテンツに関連するデータと共に記憶する。ポータブルデバイス6-3は、コンテンツに関連するデータに基づいて、記憶しているコンテンツを再生し、図示せぬヘッドフォンなどに出力する。使用者は、コンテンツを記憶したポータブルデバイス6-3をパーソナルコンピュータ1から取り外して、持ち歩き、記憶しているコンテンツを再生させて、コンテンツに対応する音楽などをヘッドフォンなどで聴くことができる。

【0038】以下、ポータブルデバイス6-1乃至6-3を個々に区別する必要があるとき、単にポータブルデバイス6と称する。

【0039】図2は、パーソナルコンピュータ1の構成を説明する図である。CPU (Central Processing Unit) 11は、各種アプリケーションプログラム（詳細については後述する）や、OS (Operating System)を実際に実行する。ROM (Read-only Memory) 12は、一般的には、CPU 11が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。RAM (Random-Access Memory) 13は、CPU 11の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはCPUバスなどから構成さ

れるホストバス14により相互に接続されている。

【0040】ホストバス14は、ブリッジ15を介して、PCI (Peripheral Component Interconnect/Interface) バスなどの外部バス16に接続されている。

【0041】キーボード18は、CPU 11に各種の指令を入力するとき、使用者により操作される。マウス19は、ディスプレイ20の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ20は、液晶表示装置またはCRT (Cathode Ray Tube) などから成り、各種情報をテキストやイメージで表示する。HDD (Hard Disk Drive) 21は、ハードディスクを駆動し、それらにCPU 11によって実行するプログラムや情報を記録または再生させる。

【0042】ドライブ22は、装着されている磁気ディスク41、光ディスク42 (CDを含む)、光磁気ディスク43、または半導体メモリ44に記録されているデータまたはプログラムを読み出して、そのデータまたはプログラムを、インターフェース17、外部バス16、ブリッジ15、およびホストバス14を介して接続されているRAM 13に供給する。

【0043】USBポート23-1には、USBケーブル7-1を介して、ポータブルデバイス6-1が接続される。USBポート23-1は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD 21、CPU 11、またはRAM 13から供給されたデータ（例えば、コンテンツまたはポータブルデバイス6-1のコマンドなどを含む）をポータブルデバイス6-1に出力する。

【0044】USBポート23-2には、USBケーブル7-2を介して、ポータブルデバイス6-2が接続される。USBポート23-2は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD 21、CPU 11、またはRAM 13から供給されたデータ（例えば、コンテンツまたはポータブルデバイス6-2のコマンドなどを含む）をポータブルデバイス6-2に出力する。

【0045】USBポート23-3には、USBケーブル7-3を介して、ポータブルデバイス6-3が接続される。USBポート23-3は、インターフェース17、外部バス16、ブリッジ15、またはホストバス14を介して、HDD 21、CPU 11、またはRAM 13から供給されたデータ（例えば、コンテンツまたはポータブルデバイス6-3のコマンドなどを含む）をポータブルデバイス6-3に出力する。

【0046】IEC (International Electrotechnical Commission) 60958端子24aを有する音声入出力インタフェース24は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。スピーカ45は、音声入出力インタフェース24から供給された音声信号を基に、コンテンツに対応する所定の音声を出

力する。

【0047】これらのキーボード18乃至音声入出力インタフェース24は、インターフェース17に接続されており、インターフェース17は、外部バス16、ブリッジ15、およびホストバス14を介してCPU11に接続されている。

【0048】通信部25は、ネットワーク2が接続され、CPU11、またはHDD21から供給されたデータ（例えば、登録の要求、またはコンテンツの送信要求など）を、所定の方式の packets に格納して、ネットワーク2を介して、送信するとともに、ネットワーク2を介して、受信した packets に格納されているデータ（例えば、認証鍵、またはコンテンツなど）をCPU11、RAM13、またはHDD21に出力する。

【0049】半導体ICとして、一体的に形成され、パーソナルコンピュータ1に装着されるアダプタ26のCPU32は、外部バス16、ブリッジ15、およびホストバス14を介してパーソナルコンピュータ1のCPU11と共働し、各種の処理を実行する。RAM33は、CPU32が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ34は、パーソナルコンピュータ1の電源がオフされた後も保持する必要があるデータを記憶する。ROM36には、パーソナルコンピュータ1から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC (Real Time Clock) 35は、計時動作を実行し、時刻情報を提供する。

【0050】通信部25およびアダプタ26は、外部バス16、ブリッジ15、およびホストバス14を介してCPU11に接続されている。

【0051】以下、USBポート23-1乃至23-3を個々に区別する必要があるとき、単に、USBポート23と称する。以下、USBケーブル7-1乃至7-3を個々に区別する必要があるとき、単にUSBケーブル7と称する。

【0052】次に、ポータブルデバイス6の構成を図3を参照して説明する。電源回路52は、乾電池51から供給される電源電圧を所定の電圧の内部電力に変換して、CPU53乃至表示部67に供給することにより、ポータブルデバイス6全体を駆動させる。

【0053】USBコントローラ57は、USBコネクタ56を介して、パーソナルコンピュータ1とUSBケーブル7を介して接続された場合、パーソナルコンピュータ1から転送されたコンテンツを含むデータを、内部バス58を介して、CPU53に供給する。

【0054】パーソナルコンピュータ1から転送されるデータは、1 packet 当たり64バイトのデータから構成され、12Mbit/secの転送レートでパーソナルコンピュータ1から転送される。

【0055】ポータブルデバイス6に転送されるデータ

は、ヘッダおよびコンテンツから構成される。ヘッダには、コンテンツID、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデックID、ファイル情報などが格納されていると共に、再生制限処理に必要な再生制限データ、開始日時、終了日時、回数制限、および再生回数カウンタなどが格納されている。コンテンツは、ATRAC3などの符号化方式で符号化され、暗号化されている。

【0056】ヘッダサイズは、ヘッダのデータ長（例えば、33バイトなど）を表し、ファイルサイズは、コンテンツのデータ長（例えば、33,636,138バイトなど）を表す。

【0057】コンテンツ鍵は、暗号化されているコンテンツを復号するための鍵であり、パーソナルコンピュータ1とポータブルデバイス6との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ1からポータブルデバイス6に送信される。

【0058】ポータブルデバイス6がUSBケーブル7を介してパーソナルコンピュータ1のUSBポート23に接続されたとき、ポータブルデバイス6とパーソナルコンピュータ1とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス6のDSP59は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読（復号）の処理を実行する。

【0059】チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ1が生成するある値（チャレンジ）に対して、ポータブルデバイス6がパーソナルコンピュータ1と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ1が生成する値は認証の処理毎に毎回変化するもので、例えば、ポータブルデバイス6が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ1は不正を検出できる。

【0060】コンテンツIDは、コンテンツに対応した、コンテンツを特定するためのIDである。

【0061】コーデックIDは、コンテンツの符号化方式に対応したIDであり、例えば、コーデックID"1"は、ATRAC3に対応し、コーデックID"0"は、MP3 (MPEG MovingPicture Experts Group) Audio Layer-3) に対応する。

【0062】ファイル名は、コンテンツに対応するパーソナルコンピュータ1が記録しているコンテンツファイル（後述する）をASCII(American National Standard Code for Information Interchange)コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲

10

20

30

40

50

名、アーティスト名、作詞者名、または作曲者名などをASCIIコードに変換したデータである。

【0063】再生制限データは、コンテンツの再生が可能な期間（すなわち、開始日時または終了日時）または回数制限（再生の回数の制限）が設定されているか否かを示すデータである。再生制限データには、回数制限が設定されているとき、“1”が割り当てられ、再生が可能な期間が設定されているとき、“2”が割り当てられ、回数制限および再生が可能な期間がいずれも設定されていないとき（いわゆる、買い取りで購入されたとき）、“0”が割り当てられる。

【0064】開始日時および終了日時は、再生制限データが“2”であるとき、再生可能期間の範囲を示すデータである。例えば、開始日時が“00040F”であり、終了日時が“00070F”であるとき、対応するコンテンツは、2000年4月15日から2000年7月15日まで、再生が可能である。

【0065】同様に、回数制限および再生回数カウンタは、再生制限データが“1”または“2”であるとき、回数制限は、そのコンテンツに対応して予め設定された再生可能な回数であり、再生回数カウンタは、そのコンテンツの再生の処理を実行したときCPU53により更新される、コンテンツが再生された回数を示す。例えば、回数制限が“02”であるとき、そのコンテンツの再生可能な回数は2回であり、再生回数カウンタが“01”であるとき、そのコンテンツが再生された回数は1回である。

【0066】例えば、再生制限データが“2”であり、開始日時が“00040F”であり、終了日時が“00070F”であり、回数制限が“02”であるとき、ポータブルデバイス6は、対応するコンテンツを、2000年4月15日から2000年7月15日までの期間において、1日2回ずつ繰り返し再生できる。

【0067】例えば、再生制限データが“1”であり、開始日時が“000000”であり、終了日時が“000000”であり、回数制限が“0a”であり、再生回数カウンタが“05”であるとき、対応するコンテンツは、再生可能な期間の制限がなく、再生可能な回数が10回であり、再生された回数が5回である。

【0068】ポータブルデバイス6が、パーソナルコンピュータ1からコンテンツと共にコンテンツの書き込み命令を受信した場合、ROM55からRAM54に読み出したメインプログラムを実行するCPU53は、書き込み命令を受け取り、フラッシュメモリコントローラ60を制御して、パーソナルコンピュータ1から受信したコンテンツをフラッシュメモリ61に書き込ませる。

【0069】フラッシュメモリ61は、約64MByteの記憶容量を有し、コンテンツを記憶する。また、フラッシュメモリ61には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納され

ている。

【0070】なお、フラッシュメモリ61は、ポータブルデバイス6にメモリカードとして着脱可能とすることができる。

【0071】使用者による、図示せぬ再生/停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ62を介してCPU53に供給されると、CPU53は、フラッシュメモリコントローラ60に、フラッシュメモリ61から、再生用コードとコンテンツとを読み出させ、DSP59に転送させる。

【0072】DSP59は、フラッシュメモリ61から転送された再生用コードに基づいてコンテンツをCRC (Cyclic Redundancy Check) 方式で誤り検出をした後、再生して、再生したデータ（図3中においてD1で示す）をデジタル/アナログ変換回路63に供給する。

【0073】DSP59は、内部に設けられた図示せぬ発信回路とともに一体に構成され、外付けされた水晶で成る発振子59AからのマスタークロックMCLKを基に、コンテンツを再生するとともに、マスタークロックMCLK、マスタークロックMCLKを基に内部の発振回路で生成した所定の周波数のビットクロックBCLK、並びにフレーム単位のLチャンネルクロックLCLK、およびRチャンネルクロックRCLKからなる動作クロックLRCLKをデジタルアナログ変換回路63に供給する。

【0074】DSP59は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをデジタルアナログ変換回路63に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロックの供給を停止して、デジタルアナログ変換回路63を停止させて、ポータブルデバイス6全体の消費電力量を低減する。

【0075】同様に、CPU53およびUSBコントローラ57も、水晶で成る発振子53Aまたは57Aがそれぞれ外付けされ、発振子53Aまたは57Aからそれぞれ供給されるマスタークロックMCLKに基づき、所定の処理を実行する。

【0076】このように構成することで、ポータブルデバイス6は、CPU53、DSP59、USBコントローラ57等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化すると共に小型化することができる。

【0077】デジタルアナログ変換回路63は、再生したコンテンツをアナログの音声信号に変換して、これを増幅回路64に供給する。増幅回路64は、音声信号を増幅して、ヘッドフォンジャック65を介して、図示せぬヘッドフォンに音声信号を供給する。

【0078】このように、ポータブルデバイス6は、図示せぬ再生/停止ボタンが押圧操作されたとき、CPU53の制御に基づいてフラッシュメモリ61に記憶されているコンテンツを再生するとともに、再生中に再生/停

止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

【0079】ポータブルデバイス6は、停止後に再度再生／停止ボタンが押圧操作されたとき、CPU53の制御に基づいて停止した位置からコンテンツの再生を再開する。再生／停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス6は、自動的に電源をオフして消費電力を低減する。

【0080】因みに、ポータブルデバイス6は、電源がオフになった後に再生／停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、1曲目から再生する。

【0081】また、ポータブルデバイス6のCPU53は、LCDコントローラ68を制御して、表示部67に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量および乾電池51の残量等の情報を表示させる。

【0082】さらに、ポータブルデバイス6は、EEPROM68に、フラッシュメモリ80に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ61のブロック位置、およびその他の種々のメモリ蓄積情報等のいわゆるFAT（File Allocation Table）を格納する。

【0083】因みに、本実施の形態においては、コンテンツは、64KByteを1ブロックとして扱われ、1曲のコンテンツに対応したブロック位置がFATに格納される。

【0084】フラッシュメモリ61にFATが格納される場合、例えば、1曲目のコンテンツがCPU53の制御によりフラッシュメモリ61に書き込まれると、1曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ61に書き込まれ、次に、2曲目のコンテンツがフラッシュメモリ61に書き込まれると、2曲目のコンテンツに対応するブロック位置がFATとしてフラッシュメモリ61（1曲目と同一の領域）に書き込まれる。

【0085】このように、FATは、フラッシュメモリ61へのコンテンツの書き込みの度に書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に2重に書き込まれる。

【0086】FATがフラッシュメモリ61に書き込まれると、1回のコンテンツの書き込みに対応して、フラッシュメモリ61の同一の領域が2回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ61に規定されている書き換えの回数に達してしまい、フラッシュメモリ61の書き換えができなくなってしまう。

【0087】そこで、ポータブルデバイス6は、FATをE

EPROM68に記憶させて、1回のコンテンツの書き込みに対応するフラッシュメモリ61の書き換えの頻度を少なくしている。

【0088】書き換えの回数の多いFATをEEPROM68に記憶させることにより、FATをフラッシュメモリ61に記憶させる場合に比較して、ポータブルデバイス6は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、CPU53は、EEPROM68にFATを追記するように書き込ませるので、EEPROM68の同一の領域の書き換えの頻度を少なくして、EEPROM68が短期間で書き換え不能になることを防止する。

【0089】ポータブルデバイス6は、USBケーブル7を介してパーソナルコンピュータ1に接続されたとき（以下、これをUSB接続と称する）、USBコントローラ57からCPU53に供給される割り込み信号に基づき、USB接続されたことを認識する。

【0090】ポータブルデバイス6は、USB接続されたことを認識すると、パーソナルコンピュータ1からUSBケーブル7を介して規定電流値の外部電力の供給を受けるとともに、電源回路52を制御して、乾電池51からの電力の供給を停止させる。

【0091】CPU53は、USB接続されたとき、DSP59のコンテンツの再生の処理を停止させる。これにより、CPU53は、パーソナルコンピュータ1から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

【0092】このようにCPU53は、USB接続されると、乾電池51から供給される電力からパーソナルコンピュータ1から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ1からの外部電力が使用され、電力単価の高い乾電池51の消費電力が低減され、かくして乾電池51の寿命を延ばすことができる。

【0093】なお、CPU53は、パーソナルコンピュータ1からUSBケーブル7を介して外部電力の供給を受けたとき、DSP59の再生処理を停止させることにより、DSP59からの輻射を低減させ、その結果としてパーソナルコンピュータ1を含むシステム全体の輻射を一段と低減させる。

【0094】図4は、CPU11の所定のプログラムの実行等により実現される、パーソナルコンピュータ1の機能の構成を説明するブロック図である。コンテンツ管理プログラム111は、EMD選択プログラム131、チェックイン／チェックアウト管理プログラム132、暗号方式変換プログラム135、圧縮方式変換プログラム136、暗号化プログラム137、利用条件変換プログラム139、利用条件管理プログラム140、認証プログラム141、復号プログラム142、PD用ドライバ143、購入用プログラム144、および購入用プログラム145などの複数のプログラムで構成されている。

【0095】コンテンツ管理プログラム111は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム111を読み出しても、インストラクションを特定できないなど）ように構成されている。

【0096】EMD選択プログラム131は、コンテンツ管理プログラム111がパーソナルコンピュータ1にインストールされるとき、コンテンツ管理プログラム111には含まれず、後述するEMDの登録の処理において、ネットワーク2を介して、EMD登録サーバ3から受信される。EMD選択プログラム131は、EMDサーバ4-1乃至4-3のいずれかとの接続を選択して、購入用アプリケーション115、または購入用プログラム144若しくは142に、EMDサーバ4-1乃至4-3のいずれかとの通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

【0097】チェックイン／チェックアウト管理プログラム132は、チェックインまたはチェックアウトの設定、およびコンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかにチェックアウトするか、またはポータブルデバイス6-1乃至6-3に記憶されているコンテンツをチェックインする。

【0098】チェックイン／チェックアウト管理プログラム132は、チェックインまたはチェックアウトの処理に対応して、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに格納されている利用条件のデータを更新する。

【0099】コピー管理プログラム133は、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかにコピーするか、またはポータブルデバイス6-1乃至6-3からコンテンツをコンテンツデータベース114にコピーする。

【0100】移動管理プログラム134は、コンテンツデータベース114に記録されている利用条件ファイル162-1乃至162-Nに基づいて、コンテンツファイル161-1乃至161-Nに格納されているコンテンツをポータブルデバイス6-1乃至6-3のいずれかに移動するか、またはポータブルデバイス6-1乃至6-3からコンテンツをコンテンツデータベース114に移動する。

【0101】暗号方式変換プログラム135は、ネットワーク2を介して、購入用アプリケーションプログラム

115がEMDサーバ4-1から受信したコンテンツの暗号化の方式、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの暗号化の方式、または購入用プログラム145がEMDサーバ4-3から受信したコンテンツの暗号化の方式を、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツと同一の暗号化の方式に変換する。

【0102】また、暗号方式変換プログラム135は、ポータブルデバイス6-1または6-3にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス6-1または6-3が利用可能な暗号化方式に変換する。

【0103】圧縮方式変換プログラム136は、ネットワーク2を介して、購入用アプリケーションプログラム115がEMDサーバ4-1から受信したコンテンツの圧縮の方式、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの圧縮の方式、または購入用プログラム145がEMDサーバ4-3から受信したコンテンツの圧縮の方式を、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツと同一の圧縮の方式に変換する。

【0104】また、圧縮方式変換プログラム136は、ポータブルデバイス6-1または6-3にコンテンツをチェックアウトするとき、チェックアウトするコンテンツを、ポータブルデバイス6-1または6-3が利用可能な圧縮の方式に変換する。

【0105】暗号化プログラム137は、例えばCDから読み取られ、録音プログラム113から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツと同一の暗号化の方式で暗号化する。

【0106】圧縮／伸張プログラム138は、例えばCDから読み取られ、録音プログラム113から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース114が記録しているコンテンツファイル161-1乃至161-Nに格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム138は、符号化されているコンテンツを伸張（復号）する。

【0107】利用条件変換プログラム139は、ネットワーク2を介して、購入用アプリケーションプログラム115がEMDサーバ4-1から受信したコンテンツの利用条件を示すデータ（いわゆる、Usage Rule）、購入用プログラム144がEMDサーバ4-2から受信したコンテンツの利用条件を示すデータ、または購入用プログラム145がEMDサーバ4-3から受信したコンテンツの利用条件を示すデータを、コンテンツデータベース11

10

20

30

40

50

4 が記録している利用条件ファイル 162-1 乃至 162-N に格納されている利用条件データと同一のフォーマットに変換する。

【0108】また、利用条件変換プログラム 139 は、ポータブルデバイス 6-1 または 6-3 にコンテンツをチェックアウトするとき、チェックアウトするコンテンツに対応する利用条件のデータを、ポータブルデバイス 6-1 または 6-3 が利用可能な利用条件のデータに変換する。

【0109】利用条件管理プログラム 140 は、コンテンツのコピー、移動、チェックイン、またはチェックアウトの処理を実行する前に、コンテンツデータベース 114 に記録されている利用条件ファイル 162-1 乃至 162-N に格納されている利用条件のデータに対応するハッシュ値（後述する）を基に、利用条件のデータの改竄を検出する。利用条件管理プログラム 140 は、コンテンツのコピー、移動、チェックイン、またはチェックアウトの処理に伴う、コンテンツデータベース 114 に記録されている利用条件ファイル 162-1 乃至 162-N に格納されている利用条件のデータを更新に対応して、利用条件のデータに対応するハッシュ値を更新する。

【0110】認証プログラム 141 は、コンテンツ管理プログラム 111 と購入用アプリケーションプログラム 115 との相互認証の処理、およびコンテンツ管理プログラム 111 と購入用プログラム 144 との相互認証の処理を実行する。また、認証プログラム 141 は、EMD サーバ 4-1 と購入用アプリケーションプログラム 115 との相互認証の処理、EMD サーバ 4-2 と購入用プログラム 144 との相互認証の処理、および EMD サーバ 4-3 と購入用プログラム 145 との相互認証の処理で利用される認証鍵を記憶している。

【0111】認証プログラム 141 が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム 111 がパーソナルコンピュータ 1 にインストールされたとき、認証プログラム 141 に記憶されておらず、表示操作指示プログラム 112 により登録の処理が正常に実行されたとき、EMD 登録サーバ 3 から供給され、認証プログラム 141 に記憶される。

【0112】復号プログラム 142 は、コンテンツデータベース 114 が記録しているコンテンツファイル 161-1 乃至 161-N に格納されているコンテンツをパーソナルコンピュータ 1 が再生するとき、コンテンツを復号する。

【0113】PD 用ドライバ 143 は、ポータブルデバイス 6-2 に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス 6-2 から所定のコンテンツをチェックインするとき、ポータブルデバイス 6-2 にコンテンツまたはポータブルデバイス 6-2 に所定の処理を実行させるコマンドを供給する。

【0114】PD 用ドライバ 143 は、ポータブルデバイス 6-1 に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス 6-1 から所定のコンテンツをチェックインするとき、デバイスドライバ 116-1 にコンテンツ、またはデバイスドライバ 116-1 に所定の処理を実行させるコマンドを供給する。

【0115】PD 用ドライバ 143 は、ポータブルデバイス 6-3 に所定のコンテンツをチェックアウトするとき、またはポータブルデバイス 6-3 から所定のコンテンツをチェックインするとき、デバイスドライバ 116-2 にコンテンツ、またはデバイスドライバ 116-2 に所定の処理を実行させるコマンドを供給する。

【0116】購入用プログラム 144 は、いわゆる、プラグインプログラムであり、コンテンツ管理プログラム 111 と共にインストールされ、EMD 登録サーバ 3 からネットワーク 2 を介して供給され、または所定の CD に記録されて供給される。購入用プログラム 144 は、パーソナルコンピュータ 1 にインストールされたとき、コンテンツ管理プログラム 111 の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム 111 とデータを送受信する。

【0117】購入用プログラム 144 は、例えば、シャッフルされているインストラクション、または暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、購入用プログラム 144 を読み出しても、インストラクションを特定できないなど）ように構成されている。

【0118】購入用プログラム 144 は、ネットワーク 2 を介して、EMD サーバ 4-2 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4-2 からコンテンツを受信する。また、購入用プログラム 144 は、EMD サーバ 4-2 からコンテンツを受信するとき、課金の処理を実行する。

【0119】購入用プログラム 145 は、コンテンツ管理プログラム 111 と共にインストールされるプログラムであり、ネットワーク 2 を介して、EMD サーバ 4-3 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4-3 からコンテンツを受信する。また、購入用プログラム 145 は、EMD サーバ 4-3 からコンテンツを受信するとき、課金の処理を実行する。

【0120】表示操作指示プログラム 112 は、フィルタリングデータファイル 181、表示データファイル 182、画像ファイル 183-1 乃至 183-K、または履歴データファイル 184 を基に、ディスプレイ 20 に所定のウィンドウの画像を表示させ、キーボード 18 またはマウス 19 への操作を基に、コンテンツ管理プログラム 111 にチェックインまたはチェックアウトなどの処理の実行を指示する。

【0121】フィルタリングデータファイル 181 は、

コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 乃至 161-N に格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、HDD 21 に記録されている。

【0122】表示データファイル 182 は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 乃至 161-N に格納されているコンテンツに対応するデータを格納して、HDD 21 に記録されている。

【0123】画像ファイル 183-1 乃至 183-K 10 は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 乃至 161-N に対応する画像、または後述するパッケージに対応する画像を格納して、HDD 21 に記録されている。

【0124】以下、画像ファイル 183-1 乃至 183-K を個々に区別する必要があるとき、単に、画像ファイル 183 と称する。

【0125】履歴データファイル 184 は、コンテンツデータベース 114 に記録されているコンテンツファイル 161-1 乃至 161-N に格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、HDD 21 に記録されている。

【0126】表示操作指示プログラム 112 は、登録の処理のとき、ネットワーク 2 を介して、EMD 登録サーバ 3 に、予め記憶しているコンテンツ管理プログラム 111 の ID を送信するとともに、EMD 登録サーバ 3 から認証用鍵および EMD 選択プログラム 131 を受信して、コンテンツ管理プログラム 111 に認証用鍵および EMD 選択プログラム 131 を供給する。

【0127】録音プログラム 113 は、所定のウィンドウの画像を表示させて、キーボード 18 またはマウス 19 への操作を基に、ドライブ 22 に装着された光ディスク 42 である CD からコンテンツの録音時間などのデータを読み出す。

【0128】録音プログラム 113 は、CD に記録されているコンテンツの録音時間などを基に、ネットワーク 2 を介して、WWW サーバ 5-1 または 5-2 に CD に対応するデータ（例えば、アルバム名、またはアーティスト名など）または CD に記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWW サーバ 5-1 または 5-2 から CD に対応するデータまたは CD に記録されているコンテンツに対応するデータを受信する。

【0129】録音プログラム 113 は、受信した CD に対応するデータまたは CD に記録されているコンテンツに対応するデータを、表示操作指示プログラム 112 に供給する。

【0130】また、録音の指示が入力されたとき、録音プログラム 113 は、ドライブ 22 に装着された光ディ 50

スク 42 である CD からコンテンツを読み出して、コンテンツ管理プログラム 111 に出力する。

【0131】コンテンツデータベース 114 は、コンテンツ管理プログラム 111 から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル 161-1 乃至 161-N のいずれかに格納する（HDD 21 に記録する）。コンテンツデータベース 114 は、コンテンツファイル 161-1 乃至 161-N にそれぞれ格納されているコンテンツに対応する利用条件のデータを、コンテンツが格納されているコンテンツファイル 161-1 乃至 161-N にそれぞれ対応する利用条件ファイル 162-1 乃至 162-N のいずれかに格納する（HDD 21 に記録する）。

【0132】コンテンツデータベース 114 は、コンテンツファイル 161-1 乃至 161-N または利用条件ファイル 162-1 乃至 162-N をレコードとして記録してもよい。

【0133】例えば、コンテンツファイル 161-1 に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル 162-1 に格納されている。コンテンツファイル 161-N に格納されているコンテンツに対応する利用条件のデータは、利用条件ファイル 162-N に格納されている。

【0134】なお、利用条件ファイル 162-1 乃至 162-N に記録されているデータは、後述する期限データベースに記録されているデータ、または曲データベースに記録されているデータに対応する。すなわち、コンテンツデータベース 114 は、後述する期限データベースおよび曲データベースを包含して、構成されている。

【0135】以下、コンテンツファイル 161-1 乃至 161-N を個々に区別する必要があるとき、単に、コンテンツファイル 161 と称する。以下、利用条件ファイル 162-1 乃至 162-N を個々に区別する必要があるとき、単に、利用条件ファイル 162 と称する。

【0136】購入用アプリケーションプログラム 115 は、EMD 登録サーバ 3 からネットワーク 2 を介して供給され、または所定の CD-ROM に記録されて供給される。購入用アプリケーションプログラム 115 は、ネットワーク 2 を介して、EMD サーバ 4-1 に所定のコンテンツの送信を要求するとともに、EMD サーバ 4-1 からコンテンツを受信して、コンテンツ管理プログラム 111 に供給する。また、購入用アプリケーションプログラム 115 は、EMD サーバ 4-1 からコンテンツを受信するとき、課金の処理を実行する。

【0137】次に、表示データファイル 82 に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル 161-1 乃至 161-N との対応付けについて説明する。

【0138】コンテンツファイル 161-1 乃至 161-N のいずれかに格納されているコンテンツは、所定の

パッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、またはフィルタリングパッケージのいずれかである。

【0139】オリジナルパッケージは、1以上のコンテンツが属し、EMDサーバ4-1乃至4-3におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、または一枚のCDに対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、または追加した情報の変更）することができる。

【0140】マイセレクトパッケージは、使用者が任意に選択した1以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、1以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

【0141】フィルタリングパッケージには、フィルタリングデータファイル181に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、EMDサーバ4-1乃至4-3またはWWWサーバ5-1若しくは5-2などからネットワーク2を介して供給され、または所定のCDに記録されて供給される。使用者は、フィルタリングデータファイル181に格納されているフィルタリングデータを編集することができる。

【0142】フィルタリングデータは、所定のコンテンツを選択する、またはコンテンツに対応する重みを算出する基準となる。例えば、今週のJ-POP（日本のポップス）ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ1は、今週の日本のポップス1位のコンテンツ乃至今週の日本のポップス10位のコンテンツを特定することができる。

【0143】フィルタリングデータファイル181は、例えば、過去1月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、または曲名に“愛”の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

【0144】このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ221（コンテンツ用表示データ221に使用者が設定したデータを含む）、または履歴データ184などと、フィルタリングデータとを対応させて選択される。

【0145】ドライバ117は、コンテンツ管理プログラム111などの制御の基に、音声入出力インターフェ

ース24を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム111に供給するか、若しくはコンテンツ管理プログラム111を介してコンテンツデータベース114から供給されたコンテンツをデジタルデータとして出力するか、または、コンテンツ管理プログラム111を介してコンテンツデータベース114から供給されたコンテンツに対応するアナログ信号を出力する。

【0146】図5は、表示操作指示プログラム112を起動させたとき、操作指示プログラム112がディスプレイ20に表示させる表示操作指示ウィンドウの例を示す図である。

【0147】表示操作指示ウィンドウには、録音プログラム113を起動させるためのボタン201、EMD選択プログラム131を起動させるためのボタン202、チェックインまたはチェックアウトの処理の設定を行うフィールドを表示させるためのボタン203、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン204等が配置されている。

【0148】ボタン205が選択されているとき、フィールド211には、オリジナルパッケージに対応するデータが表示される。ボタン206が選択されているとき、フィールド211には、マイセレクトパッケージに対応するデータが表示される。ボタン207が選択されているとき、フィールド211には、フィルタリングパッケージに対応するデータが表示される。

【0149】フィールド211に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、またはアーティスト名などである。

【0150】例えば、図5においては、パッケージ名称“ファースト”およびアーティスト名“A太郎”、およびパッケージ名称“セカンド”およびアーティスト名“A太郎”などがフィールド211に表示される。

【0151】フィールド212には、フィールド211で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド212に表示されるデータは、例えば、曲名、演奏時間、またはチェックアウト可能回数などである。

【0152】例えば、図5においては、パッケージ名称“セカンド”に対応するパッケージが選択されているので、パッケージ名称“セカンド”に対応するパッケージに属するコンテンツに対応する曲名“南の酒場”およびチェックアウト可能回数（例えば、8分音符の1つがチェックアウト1回に相当し、8分音符が2つでチェックアウト2回を示す）、並びに曲名“北の墓場”およびチェックアウト可能回数（8分音符が1つでチェックアウト1回を示す）などがフィールド212に表示される。

【0153】このように、フィールド212に表示されるチェックアウト可能回数としての1つの8分音符は、

10

20

30

40

50

対応するコンテンツが1回チェックアウトできることを示す。

【0154】フィールド212に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が0である。（ただし、パーソナルコンピュータ1はそのコンテンツを再生することができる。））ことを示す。また、フィールド212に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限が無い（何度でも、チェックアウトできる）ことを示している。

【0155】なお、チェックアウト可能回数は、図5に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等で表示してもよい。

【0156】また、表示操作指示ウィンドウには、選択されているパッケージまたはコンテンツに対応付けられている画像等（図4の画像ファイル183-1乃至183-Kのいずれかに対応する）を表示させるフィールド208が配置されている。ボタン209は、選択されているコンテンツを再生する（コンテンツに対応する音声

をスピーカ45に出力させる）とき、クリックされる。

【0157】ボタン205が選択され、フィールド211に、オリジナルパッケージに対応するデータが表示されている場合、フィールド212に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111に、選択されている曲名に対応する、コンテンツデータベース114に格納されている所定のコンテンツを消去させる。

【0158】録音プログラム113が表示させるウィンドウのボタン（後述するボタン255）が選択されて（アクティブにされて）いる場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス6-1乃至6-3のいずれかに記憶されているコンテンツの曲名を表示するフィールド213を表示する。

【0159】録音プログラム113が表示させるウィンドウのボタンが選択されている場合、CDから読み出したコンテンツがコンテンツデータベース114に記録されたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111に、コンテンツデータベース114に記録した、CDから読み出したコンテンツを予め指定されているポータブルデバイス6-1乃至6-3のいずれかにチェックアウトさせる。

【0160】フィールド213にはコンテンツの曲名に対応させて、フィールド213の最も左に、そのコンテンツがパーソナルコンピュータ1にチェックインできるか否かを示す記号が表示される。例えば、フィールド2

13の最も左に位置する“○”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ1にチェックインできる（すなわち、パーソナルコンピュータ1からチェックアウトされた）ことを示している。フィールド213の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ1にチェックインできない（すなわち、パーソナルコンピュータ1からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた）ことを示している。

【0161】表示操作指示プログラム112が表示操作指示ウィンドウにフィールド213を表示させたとき、表示操作指示プログラム112は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス6-1乃至6-3のいずれかに記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス6-1乃至6-3のいずれかに記憶されているコンテンツが属するパッケージ）の名称を表示するフィールド214、フィールド213を閉じるためのボタン210、およびチェックインまたはチェックアウトを実行させるボタン215を表示する。

【0162】更に、表示操作指示プログラム112が表示操作指示ウィンドウにフィールド213を表示させたとき、表示操作指示プログラム112は、表示操作指示ウィンドウに、フィールド212で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン216、フィールド213で選択された曲名に対応するコンテンツのチェックインを設定するボタン217、フィールド213に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン218、およびチェックインまたはチェックアウトの設定を取り消すボタン219を配置させる。

【0163】ボタン216乃至219の操作によるチェックインまたはチェックアウトの設定だけでは、パーソナルコンピュータ1は、チェックインまたはチェックアウトの処理を実行しない。

【0164】ボタン216乃至219の操作によるチェックインまたはチェックアウトの設定をした後、ボタン215がクリックされたとき、表示操作指示プログラム112は、コンテンツ管理プログラム111にチェックインまたはチェックアウトの処理を実行させる。すなわち、ボタン215がクリックされたとき、表示操作指示プログラム112は、チェックインまたはチェックアウトの設定に基づき、コンテンツ管理プログラム111に、ポータブルデバイス6-1乃至6-3のいずれかにコンテンツを送信させるか、またはチェックインに対応する所定のコマンド（例えば、ポータブルデバイス6-1乃至6-3のいずれかが記憶している所定のコンテンツを消去させるコマンドなど）を送信させるとともに、送信したコンテンツまたはコマンドに対応する利用条件

ファイル 162 に格納されている利用条件のデータを更新させる。

【0165】チェックインまたはチェックアウトが実行されたとき、表示操作指示プログラム 112 は、送信したコンテンツまたは送信されたコマンドに対応して、履歴データファイル 184 に格納されている履歴データを更新する。履歴データは、チェックインまたはチェックアウトされたコンテンツを特定する情報、またはそのコンテンツがチェックインまたはチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス 6-1 乃至 6-3 の名称などから成る。

【0166】チェックインまたはチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェックインまたはチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックインまたはチェックアウトの処理の回数を減らして、チェックインまたはチェックアウトに必要な時間全体（設定および実行を含む）を短くすることができる。

【0167】図 6 は、録音プログラム 113 がディスプレイ 20 に表示させるウィンドウの例を説明する図である。例えば、WWWサーバ 5-2 から受信した CD の情報を基に、録音プログラム 113 は、フィールド 251 に、“アシンクロナイズド”などの CD のタイトルを表示する。WWWサーバ 5-2 から受信した CD の情報を基に、録音プログラム 113 は、フィールド 252 に、例えば、“クワイ”などのアーティスト名を表示する。

【0168】WWWサーバ 5-2 から受信した CD の情報を基に、録音プログラム 113 は、フィールド 253 の曲名を表示する部分に、例えば、“ヒート”、“ブラネット”、“ブラック”、“ソウル”などの曲名を表示する。同様に、録音プログラム 113 は、フィールド 253 のアーティストを表示する部分に、例えば、“クワイ”などのアーティスト名を表示する。

【0169】録音プログラム 113 が所定の CD の情報を受信した後、録音プログラム 113 は、HDD 21 の所定のディレクトリに CD の情報を格納する。

【0170】ボタン 254 などがクリックされて、CD の情報の取得の指示を受けたとき、録音プログラム 113 は、始めに、HDD 21 の所定のディレクトリを検索する。録音プログラム 113 は、そのディレクトリに CD の情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されている CD の情報を利用するか否かを選択させる。

【0171】録音プログラム 113 が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン 256 がクリックされたとき、録音プログラム 113 は、ドライブ 22 に格納されている CD からコンテンツを読み出して、CD から読み出したコンテンツを CD の情報と共にコンテンツ管理プログラム 111 に供給する。コンテンツ管理プログラム 111 の圧縮／伸張プロ

グラム 138 は、録音プログラム 113 から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム 137 は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム 139 は、圧縮され、暗号化されたコンテンツに対応する利用条件のデータを生成する。

【0172】コンテンツ管理プログラム 111 は、圧縮され、暗号化されたコンテンツを利用条件のデータと共に、コンテンツデータベース 114 に供給する。

【0173】コンテンツデータベース 114 は、コンテンツ管理プログラム 111 から受信したコンテンツに対応するコンテンツファイル 161 および利用条件ファイル 162 を生成して、コンテンツファイル 161 にコンテンツを格納するとともに、利用条件ファイル 162 に利用条件のデータを格納する。

【0174】コンテンツ管理プログラム 111 は、コンテンツデータベース 114 にコンテンツおよびコンテンツに対応する利用条件のデータが格納されたとき、録音プログラム 113 から受信した CD の情報および利用条件のデータを表示操作指示プログラム 112 に供給する。

【0175】表示操作指示プログラム 112 は、録音の処理でコンテンツデータベース 114 に格納されたコンテンツに対応する利用条件のデータおよび CD の情報を基に、表示データファイル 182 に格納する表示用のデータを生成する。

【0176】録音プログラム 113 が表示させるウィンドウには、更に、CD から読み出したコンテンツをコンテンツデータベース 114 に記録したとき、自動的に、CD から読み出したコンテンツをポータブルデバイス 6-1 乃至 6-3 のいずれかにチェックアウトさせるか否かの設定を行うボタン 255 が配置されている。

【0177】例えば、ボタン 255 がクリックされたとき、録音プログラム 113 は、ポータブルデバイス 6-1 乃至 6-3 のリストを示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス 6-1 乃至 6-3 のいずれかを選択したとき、パーソナルコンピュータ 1 は、選択されたポータブルデバイス 6-1 乃至 6-3 のいずれかに、自動的に、CD から記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから“チェックアウトしない”を選択した場合、パーソナルコンピュータ 1 は、CD からコンテンツを記録したとき、チェックアウトしない。

【0178】このように、録音プログラム 113 が表示させるウィンドウのボタン 255 をアクティブにしておくだけで、CD から読み出したコンテンツがコンテンツデータベース 114 に記録されたとき、パーソナルコンピュータ 1 は、予め指定されているポータブルデバイス 6-1 乃至 6-3 のいずれかに、CD から読み出したコンテンツをチェックアウトさせることができる。

10

20

30

40

50

【0179】次に、図7のフローチャートを参照して、コンテンツ管理プログラム111、表示操作指示プログラム112、録音プログラム113、およびコンテンツデータベース114を実行するCPU11による、ドライブ22に装着されたCDから再生したコンテンツをHDD21に転送し、コピーする場合の処理について説明する。使用者がキーボード18またはマウス19を操作して、インタフェース17を介してCPU11に対してドライブ22に装着されたCD（図示せず）から再生されたコンテンツをHDD21に転送、コピーする指令を入力すると、録音プログラム113は、ステップS11において、インタフェース17を介してディスプレイ20にコピーするコンテンツを選択するための、例えば、図6に示すGUI（Graphical User Interface）を表示させる。

【0180】具体的には、例えば、録音プログラム113は、ドライブ22に装着されたCDのTOC（Table Of Contents）を読み込み、そのCDに含まれるコンテンツの情報を得て、ディスプレイ20に表示させる。または、録音プログラム113は、CDに含まれている各コンテンツ毎のISRC（International Standard Recording Code）を読み出し、そのコンテンツの情報を得て、ディスプレイ20に表示させる。あるいはまた、ボタン254がクリックされたとき、録音プログラム113は、ネットワーク2を介してWWWサーバ5-1または5-2にアクセスし、TOCを用いて、そのCDのコンテンツの情報を得て、コンテンツに対応する曲名などをフィールド253に表示させる。

【0181】使用者は、ディスプレイ20のGUIを利用してキーボード18またはマウス19を操作し、フィールド253に表示されている曲名に対応するチェックボックスをクリックするなどして、コピーするコンテンツを選択する。

【0182】次に、ステップS12において、録音プログラム113は、利用条件管理プログラム140に、HDD21に格納されている期限データベース（図4に示すコンテンツデータベース114の利用条件ファイル162-1乃至162-Nに対応する）をチェックさせる。この期限データベースチェック処理の詳細は、図8のフローチャートに示されている。

【0183】ステップS31において利用条件管理プログラム140は、アダプタ26のCPU32と共働して、期限データベース全体のハッシュ値を計算し、ステップS32において、その計算された値と、前回保存しておいたハッシュ値と比較する。

【0184】なお、期限データベースにデータが何ら記録されていないとき、利用条件管理プログラム140は、ハッシュ値を計算しない。

【0185】すなわち、HDD21には、期限データベースが形成されており、この期限データベースには、図9に示すように、HDD21に記録されているコンテンツ

（コンテンツ）を管理する管理情報として、過去に記録されたことのあるコンテンツのISRCとコピー日時が対応して記憶されている。この例においては、アイテム1乃至アイテム3の3つのアイテムについて、それぞれのISRCとコピー日時が記憶されている。この期限データベースに記録されている全てのコンテンツのISRCとコピー日時に基づいた期限データベース全体のハッシュ値が、後述するように、ステップS38において、アダプタ26のCPU32により計算され、不揮発性メモリ34に記憶されている。ハッシュ値は、データに対してハッシュ関数を適用して得られた値である。

【0186】ハッシュ関数は、任意の長さのメッセージを固定長に短く圧縮した値にマップする一方向性の関数であり、圧縮したデータからもとのデータを求める逆変換が困難な性質を持つものである。また、ハッシュ値同士の衝突が起こりにくく、即ち、例えば違う二つのメッセージに対して同じ値を付けることを困難にするものである。ハッシュ関数は、メッセージが通信途中で改竄されなかったことを確認するためのチェックサムとして用いられ、デジタル署名の中で用いられる。ハッシュ関数の例としては、SHA（Secure Hash Algorithm）、MD（Message Digest）5などがある。

【0187】利用条件管理プログラム140は、ステップS31において、CPU32が実行したのと同様にハッシュ値を計算する。そして、ステップS32において、利用条件管理プログラム140は、CPU32に、不揮発性メモリ34に記憶されているハッシュ値の読み出しを要求し、転送を受けたハッシュ値と、ステップS31で、いま自分自身が計算したハッシュ値とを比較する。

【0188】ステップS33において、利用条件管理プログラム140は、ステップS31でいま計算したハッシュ値と、不揮発性メモリ34に記憶されている前回の期限データベースのハッシュ値とが一致するか否かを判定し、一致しない場合には、期限データベースが改竄されたものと判定し、利用条件管理プログラム140は、ステップS34において、例えば、録音プログラム113に「期限データベースが改竄されたので、コピーができません」といったメッセージを発生させ、インタフェース17を介してディスプレイ20に出力させ、表示させ、以後、処理を終了させる。すなわち、この場合には、CDに記録されているコンテンツを再生し、HDD21にコピーする処理が禁止される。

【0189】ステップS31で計算したハッシュ値と、前回のハッシュ値とが一致する場合には、ステップS35に進み、利用条件管理プログラム140は、録音プログラム113に、ステップS11で指定されたコピーするコンテンツとして選択されたコンテンツ（選択されたコンテンツ）のISRCをCDから取得させる。CDにISRCが記録されていない場合、利用条件管理プログラム140は、録音プログラム113に、そのCDのTOCのデータを

読み出させ、そのデータにハッシュ関数を適用するなどして、例えば、58ビットなどの適当な長さのデータを得て、これをISRCに代えて用いる。

【0190】ステップS36において、利用条件管理プログラム140は、ステップS35で取得したISRC（すなわち、選択されたコンテンツ）が期限データベース

（図9）に登録されているか否かを判定する。ISRCが期限データベースに登録されていない場合には、そのコンテンツはまだHDD21に記録されていないことになるので、ステップS37に進み、利用条件管理プログラム140は、そのコンテンツのISRCと現在の日時とを期限データベースに登録する。なお、利用条件管理プログラム140は、この現在の日時として、CPU32から転送を受けた、アダプタ26のRTC35が出力する値を利用する。そして、ステップS38において、利用条件管理プログラム140は、その時点における期限データベースのデータを読み出し、アダプタ26のCPU32に転送する。CPU32は、転送されてきたデータのハッシュ値を計算し、不揮発性メモリ34に保存してする。上述したように、このようにして保存されたハッシュ値が、ステップS32において、前回保存しておいたハッシュ値として利用される。

【0191】次に、ステップS39において、利用条件管理プログラム140は、選択されたコンテンツが期限データベースに登録されていないことを表す未登録のフラグを設定する。このフラグは、後述する図7のステップS13において、選択されたコンテンツが期限データベースに登録されているか否かの判定を行うときに用いられる。

【0192】ステップS36において、選択されたコンテンツのISRCが期限データベースに登録されていると判定された場合、その選択されたコンテンツは、少なくとも一度、HDD21に登録されたことがあるコンテンツであるということになる。そこで、この場合、ステップS40に進み、利用条件管理プログラム140は、期限データベースに登録されているその選択されたコンテンツの登録日時より、現在の日時（アダプタ26のRTC35が出力した現在の日時）が48時間以上経過しているか否かを判定する。現在時刻が、登録日時より、既に48時間以上経過している場合には、HDD21に、少なくとも一度は記録したことがあるが、既に、その時から48時間以上経過しているので、そのコンテンツを再度コピーさせたとしても、コンテンツの大量のコピーは実質的に不可能なので、この場合には、HDD21へのコピーが許容される。そこで、ステップS41に進み、利用条件管理プログラム140は、期限データベースの日時を、過去の登録日時から現在の日時（RTC35の出力する日時）に変更させる。そして、ステップS38に戻り、利用条件管理プログラム140は、再び、期限データベース全体のハッシュ値をCPU32に計算させ、不揮発性メ

モリ34に保存させるとともに、ステップS39において、そのコンテンツに対して未登録のフラグを設定する。

【0193】一方、ステップS40において、現在時刻が登録日時より、まだ48時間以上経過していないと判定された場合、その選択されたコンテンツのHDD21へのコピーが禁止される。そこで、この場合には、ステップS42に進み、利用条件管理プログラム140は、その選択されたコンテンツに対応して登録済みのフラグを設定する。

【0194】ステップS40の処理により、所定の時間が経過しなければ、コンテンツの新たなコピーを生成できないので、不正でない通常の使用を目的としたコンテンツのコピーの生成を不当に妨げることなく、例えば、不正な販売または配布などに必要な大量のコンテンツのコピーの生成は、実質的に不可能となる。なお、ステップS40においては、判定の基準は48時間以上の経過としたが、48時間に限らず、例えば、12時間乃至168時間のいずれかの時間であればよい。

【0195】以上のようにして、期限データベースチェック処理により、選択されたコンテンツがHDD21に登録されているか否かを表すフラグが設定される。

【0196】図7に戻り、ステップS13においてコピー管理プログラム133は、選択されたコンテンツが期限データベースに登録済みであるか否かを、上述したフラグから判定する。選択されたコンテンツが登録済みである場合には、ステップS14に進み、コピー管理プログラム133は、録音プログラム113に、例えば、「この曲は一度コピーされてからまだ48時間以上経過していないので、コピーすることができません」のようなメッセージをディスプレイ20に表示させる。これにより、使用者は、そのコンテンツをHDD21にコピーすることができない理由を知ることができる。

【0197】ステップS13において、選択したコンテンツが期限データベースに登録されていないと判定された場合、ステップS15に進み、録音プログラム113は、ドライブ22を制御し、そこに装着されているCDからコンテンツを読み出させる。このコンテンツには、図10に示すように、所定の位置にウォーターマークコードが挿入されている。録音プログラム113は、ステップS16において、コンテンツに含まれているウォーターマークコードを抽出し、そのウォーターマークコードがコピー禁止を表しているか否かをステップS17において判定する。ウォーターマークコードがコピー禁止を表している場合には、ステップS18に進み、コピー管理プログラム133は、録音プログラム113に例えば、「コピーは禁止されています」のようなメッセージをインタフェース17を介してディスプレイ20に表示させ、コピー処理を終了させる。

【0198】これに対して、ステップS17において、

10

20

30

40

50

ウォータマークがコピー禁止を表していないと判定された場合、ステップS19に進み、録音プログラム113は、コンテンツを、圧縮／伸張プログラム138に、例えば、ATRAC (Adaptive Transform Acoustic Coding) 3 (商標) などの方式で、ソフトウェア処理により圧縮させる。ステップS20において、録音プログラム113は、暗号化プログラム137に、予め設定され、メモリ13に記憶されている暗号鍵を用いて、例えば、DES (Data Encryption Standard) 方式、FEAL (Fast Encryption Algorithm) 方式などの暗号化方法により、コンテンツを暗号化させる。暗号鍵は、この他、例えば、ソフトウェアにより発生した乱数、あるいはアダプタ26のCPU32により発生させた乱数に基づいて生成したものを用いることもできる。このように、パーソナルコンピュータ1だけではなく、それに付随して装着されたハードウェアとしてのアダプタ26のCPU32と、共働して暗号化処理を実行するようにすることで、解読がより困難となる暗号化を行うことが可能となる。

【0199】次に、ステップS21において、録音プログラム113は、暗号化されたデータを、コンテンツデータベース114に転送し、1つのファイル (コンテンツファイル161として) としてファイル名を付けてHDD21に保存させる。あるいはまた、1つのファイルの一部として、そのファイル名の位置情報 (例えば、先頭からのバイト数) を与えて保存するようにしてもよい。

【0200】この保存処理と、上記した圧縮符号化処理および暗号化処理とは別々に行うようにしてもよいし、同時に平行的に行うようにしてもよい。

【0201】さらに、ステップS22において、録音プログラム113は、暗号化プログラム137に、予め定められている不揮発性メモリ34に記憶されている保存用鍵を使って、上述したDES方式、FEAL方式などの方式で、コンテンツを暗号化した暗号鍵を暗号化させ、HDD21の曲データベース (図4に示すコンテンツデータベース114の利用条件ファイル162-1乃至162-Nに対応する) に保存する。

【0202】ステップS23において、録音プログラム113は、保存したファイルに関する情報、暗号化された暗号鍵、そのコンテンツの情報、使用者がGUIを介して入力した曲名の情報の要素を組にしてHDD21の曲データベースに登録する (利用条件ファイル162-1乃至162-Nとして記録する)。そして、ステップS24において、録音プログラム113は、CPU32に、曲データベース全体のハッシュ値を計算させ、不揮発性メモリ34に保存させる。

【0203】このようにして、例えば、図11に示すような曲データベースが、HDD21上に登録される。この例においては、アイテム1乃至アイテム3のファイル名、暗号化された暗号鍵、曲名、長さ、再生条件 (開始日時、終了日時、回数制限)、再生回数カウンタ、再生

時課金条件、コピー条件 (回数)、コピー回数カウンタ、およびコピー条件 (SCMS) が記録されている。

【0204】例えば、SDMI (Secure Digital Music Initiative) が規定する方式では、CDからコピーしたコンテンツに対応して、そのコンテンツがチェックアウトできる回数は、3回に設定される。

【0205】CDからHDD21にコンテンツが複製されて一定期間が経過すると、再びコンテンツを複製することができるようにしたので、ユーザの個人の使用の範囲とされる、数回の複製が可能となる。一方、個人の使用の範囲を超えて、例えば、大量に複製しようとする、莫大な時間が必要とされ、現実的に不可能になる。また、例えば、パーソナルコンピュータ1が故障して、HDD21に記録されていたコンテンツが消去された場合においても、一定期間の経過後、消去されたコンテンツを再び複製し、HDD21に記録することができる。

【0206】また、例えば、ネットワーク2を介してHDD21に記録されている期限データベースの内容を共有することもできる。

【0207】以上においては、ISRCに対応して複製された日時が記憶されている場合を例として説明したが、コンテンツやCDを識別する情報であれば、他のもの (例えば、曲名、アルバム名、それらの組み合わせなど) を利用することもできる。

【0208】次に、図12乃至図14のフローチャートを参照して、表示操作指示プログラム112およびコンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU52による、HDD21からポータブルデバイス6のフラッシュメモリ61 (例えば、メモリースティック (商標)) に、コンテンツを移動する処理およびチェックアウトの処理について説明する。

【0209】始めに、コンテンツの移動の処理について説明する。ステップS51において、移動管理プログラム134は、利用条件管理プログラム140に、曲データベース全体のハッシュ値を計算させ、ステップS52で、前回CPU32に計算させ、不揮発性メモリ34に保存しておいたハッシュ値と比較する。両者が一致しない場合、移動管理プログラム134は、ステップS53に進み、表示操作指示プログラム112に、例えば、「曲データベースが改竄された恐れがあります」のようなメッセージをディスプレイ20に表示させた後、処理を終了させる。この場合の処理は、図8のステップS31乃至ステップS34の処理と同様の処理である。この場合においては、HDD21からポータブルデバイス6へのコンテンツの移動が実行されないことになる。

【0210】次に、ステップS54において、移動管理プログラム134は、HDD21に形成されている曲データベース (コンテンツデータベース114に含まれる) から、そこに登録されているコンテンツの情報を読み出

10

20

30

40

50

し、表示操作指示プログラム112に、選択のためのGUIとしてディスプレイ20に表示させる。使用者は、この選択のためのGUIに基づいて、HDD21からポータブルデバイス6へ移動させるコンテンツを、図5のフィールド212に表示される曲名、ボタン216などをクリックして選択する。次に、ステップS55において、移動管理プログラム134は、ステップS54で選択された選択されたコンテンツの再生条件、コピー条件、再生時課金条件などを調べる。この処理の詳細は、図15のフローチャートを参照して後述する。

【0211】次に、ステップS56において、パーソナルコンピュータ1の認証プログラム141とポータブルデバイス6のCPU53との間において、相互認証処理が行われ、通信用鍵が共有される。

【0212】例えば、ポータブルデバイス6のフラッシュメモリ61（または、EEPROM68）には、マスター鍵KMが予め記憶されており、パーソナルコンピュータ1のRAM13（または、HDD21の所定のファイル）には、個別鍵KPとIDが予め記憶されているものとする。CPU53は、認証プログラム141から、RAM13に予め記憶されているIDの供給を受け、そのIDと自分自身が有するマスター鍵KMにハッシュ関数を適用して、RAM13に記憶されているパーソナルコンピュータ1の個別鍵と同一の鍵を生成する。このようにすることで、パーソナルコンピュータ1とポータブルデバイス6の両方に、共通の個別鍵が共有されることになる。この個別鍵を用いてさらに、一時的な通信用鍵を生成することができる。

【0213】あるいはまた、パーソナルコンピュータ1のRAM13にIDとマスター鍵KMPを予め記憶させておくとともに、ポータブルデバイス6のフラッシュメモリ61にもポータブルデバイス6のIDとマスター鍵KMMを記憶させておく。そして、それぞれのIDとマスター鍵をお互いに他方に送信することで、他方は一方から送信されてきたIDとマスター鍵にハッシュ関数を適用して、他方の個別鍵を生成する。そして、その個別鍵から、一時的な通信用鍵をさらに生成するようにする。

【0214】なお、認証の方法としては、例えば、IOS (International Organization for Standardization) 9798-2を利用することができる。

【0215】相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、ステップS57において、移動管理プログラム134は、コンテンツデータベース114に、選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツ（例えば、図7のステップS20の処理で暗号化されている）をHDD21から読み出す。ステップS58において、移動管理プログラム134は、ステップS57で読み出したデジタルデータであるコンテンツの圧縮符号化方式（ステップS19の処理）、暗号化方式（ステップS20の処理）、フォーマ

ット（例えば、ヘッダの方式など）などをポータブルデバイス6のものに変換する処理を実行する。この変換処理の詳細は、図17のフローチャートを参照して後述する。

【0216】ステップS59において、移動管理プログラム134は、PD用ドライバ143に、ステップS58で変換したコンテンツを、USBポート23を介してポータブルデバイス6に転送させる。ステップS60において、ポータブルデバイス6のCPU53は、USBコネクタ56を介してこの伝送されてきたコンテンツを受信すると、そのコンテンツを、そのままフラッシュメモリ61に記憶させる。

【0217】ステップS61において、移動管理プログラム134は、さらに、利用条件変換プログラム139に、曲データベースに登録されているその選択されたコンテンツの再生条件（開始日時、終了日時、回数制限など）を、ポータブルデバイス6が管理している形式に変換する。ステップS62において、移動管理プログラム134は、さらに、利用条件変換プログラム139に、選択されたコンテンツの曲データベース中に登録されているコピー条件中のSCMS情報を、ポータブルデバイス6の管理する形式に変換させる。そして、ステップS63において、移動管理プログラム134は、PD用ドライバ143に、ステップS61で変換した再生条件と、ステップS62で変換したSCMS情報を、ポータブルデバイス6に転送させる。ポータブルデバイス6のCPU53は、転送を受けた再生条件とSCMS情報を、フラッシュメモリ61に保存する。

【0218】ステップS64において、移動管理プログラム134はまた、PD用ドライバ143に、選択されたコンテンツの曲データベース中に登録されている再生条件、再生時課金条件、コピー条件などを、CPU11が曲データベース中で扱っている形式のまま、ポータブルデバイス6に転送させ、フラッシュメモリ61に保存させる。

【0219】ステップS65において、移動管理プログラム134は、コンテンツデータベース114に、選択されたコンテンツの暗号化されている暗号鍵を曲データベースから読み出させ、ステップS66において、復号プログラム142に、その暗号鍵をRAM13に保存されている保存用鍵で復号させ、暗号化プログラム137に通信用鍵で暗号化させる。そして、通信用鍵で暗号化した暗号鍵を、移動管理プログラム134は、PD用ドライバ143に、ポータブルデバイス6へ転送させる。

【0220】ポータブルデバイス6のCPU53は、ステップS67で、パーソナルコンピュータ1から転送されてきた暗号鍵を相互認証処理で共有した通信用鍵を用いて復号し、自分自身の保存用鍵を用いて暗号化し、既に保存したデータと関連付けて、フラッシュメモリ61に保存する。

【0221】CPU53は、暗号鍵の保存が完了すると、ステップS68において、パーソナルコンピュータ1に対して暗号鍵を保存したことを通知する。パーソナルコンピュータ1の移動管理プログラム134は、ポータブルデバイス6からこの通知を受けると、ステップS69において、コンテンツデータベース114に、そのコンテンツに対応するコンテンツファイル161を削除させるとともに、曲データベースからそのコンテンツの要素の組（すなわち、利用条件ファイル162）を削除させる。すなわち、これにより、コピーではなく、移動（ムーブ）が行われることになる。そして、ステップS70において、移動管理プログラム134は、アダプタ26のCPU32に、曲データベースのデータを転送し、全体のハッシュ値を計算させ、不揮発性メモリ34に保存させる。このハッシュ値が、上述したステップS52において、前回保存しておいたハッシュ値として用いられることになる。

【0222】次に、パーソナルコンピュータ1からポータブルデバイス6にコンテンツをチェックアウトする処理について説明する。パーソナルコンピュータ1からポータブルデバイス6にコンテンツをチェックアウトする処理は、図12乃至図14のパーソナルコンピュータ1からポータブルデバイス6へコンテンツを移動させる場合と同様の処理である。すなわち、チェックアウトの処理は、パーソナルコンピュータ1においてチェックイン／チェックアウト管理プログラム132により実行され、図14のステップS69において、コンテンツを削除する処理に代えて、曲データベースに記録されている、チェックアウトされたコンテンツのチェックアウトした回数（またはチェックアウトできる回数）を更新する処理を実行することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

【0223】次に、コンテンツ管理プログラム111を実行するCPU11による、図12のステップS55における選択されたコンテンツの再生条件などのチェック処理について図15のフローチャートを参照して説明する。ステップS81において、移動管理プログラム134は、コンテンツデータベース114に、曲データベースから、各種の条件を読み出させる。移動管理プログラム134は、ステップS82において、ステップS81で読み出した各種条件のうち、コピー回数がコピー制限回数を既に過ぎていないかを判定する。コピー回数が、コピー制限回数を既にすぎている場合には、それ以上コピーを許容する訳にはいかないので、ステップS83に進み、移動管理プログラム134は、表示操作指示プログラム112に、例えば、「既にコピー回数がコピー制限回数に達しています」のようなメッセージをディスプレイ20に表示させ、処理を終了させる。ステップS82において、コピー回数がコピー制限回数を過ぎて

いないと判定された場合、ステップS84に進み、現在日時が再生終了日時を過ぎているか否かの判定が行われる。現在日時としては、アダプタ26のRTC35より出力されたものが用いられる。これにより、使用者が、パーソナルコンピュータ1の現在時刻を意図的に過去の値に修正したものが用いられるようなことが防止される。移動管理プログラム134は、この現在日時をCPU32から提供を受けて、ステップS84の判断を自ら行うか、または、ステップS81で、曲データベースから読み出した再生条件をアダプタ26のCPU32に供給し、CPU32に、ステップS84の判定処理を実行させる。

【0224】現在日時が再生終了日時を過ぎている場合、ステップS85に進み、移動管理プログラム134は、コンテンツデータベース114に、選択されたコンテンツをHDD21から消去させるとともに、曲データベースから、その選択されたコンテンツの情報を消去させる。ステップS86において、移動管理プログラム134は、CPU32に、曲データベースのハッシュ値を計算させ、それを不揮発性メモリ34に保存させる。以後、処理は終了される。従って、この場合、コンテンツの移動が実行されない。

【0225】ステップS84において、現在日時が、再生終了日時を過ぎていないと判定された場合、ステップS87に進み、移動管理プログラム134は、その選択されたコンテンツの再生時課金条件（例えば、再生1回当たりの料金）が曲データベース中に登録されているか否かを判定する。再生時課金条件が登録されている場合には、移動管理プログラム134は、ステップS88において、PD用ドライバ143に、ポータブルデバイス6と通信させ、ポータブルデバイス6に課金機能が存在するか否かを判定する。ポータブルデバイス6に課金機能が存在しない場合には、選択されたコンテンツをポータブルデバイス6に転送する訳にはいかないので、ステップS89において、移動管理プログラム134は、表示操作指示プログラム112に、例えば、「転送先が課金機能を有していません」のようなメッセージをディスプレイ20に表示させ、コンテンツの移動処理を終了させる。

【0226】ステップS87において再生時課金条件が登録されていないと判定された場合、または、ステップS88において、ポータブルデバイス6に課金機能が存在すると判定された場合、ステップS90に進み、移動管理プログラム134は、選択されたコンテンツに関し、例えば、再生制限回数などのその他の再生条件が登録されているか否かを判定する。その他の再生条件が登録されている場合には、ステップS91に進み、移動管理プログラム134は、ポータブルデバイス6に、その再生条件を守る機能が存在するか否かを判定する。ポータブルデバイス6が、その再生条件を守る機能を有していない場合には、ステップS92に進み、移動管理プロ

グラム134は、表示操作指示プログラム112に、例えば、「転送先の装置が再生条件を守る機能を有していません」のようなメッセージをディスプレイ20に表示させ、処理を終了させる。

【0227】ステップS90において、再生条件が登録されていないと判定された場合、またはステップS91において、ポータブルデバイス6が再生条件を守る機能を有していると判定された場合、再生条件等のチェック処理が終了され、図12のステップS56に戻る。

【0228】図16は、ポータブルデバイス6が管理している（守ることが可能な）再生条件の例を表している。図16に示す再生情報は、例えば、EEPROM68に記憶されている。この例においては、アイテム1乃至アイテム3の各コンテンツについて、再生開始日時と再生終了日時が登録されているが、再生回数は、アイテム2についてのみ登録されており、アイテム1とアイテム3については登録されていない。従って、アイテム2のコンテンツが選択されたコンテンツとされた場合、再生回数の再生条件は守ることが可能であるが、アイテム1またはアイテム3のコンテンツが選択されたコンテンツとされた場合、再生回数の条件は守ることができないことになる。

【0229】次に、図17のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、図12のステップS58におけるフォーマット変換処理の詳細について説明する。ステップS101において、移動管理プログラム134は、コンテンツデータベース114に記録されている選択されたコンテンツのフォーマット（例えば、再生条件、使用条件、コピー条件などを含むヘッダなどの方式）を調べる。ステップS102において、移動管理プログラム134は、相手先の機器（今の場合、ポータブルデバイス6）に設定することが可能な条件を調べる。すなわち、移動管理プログラム134は、ポータブルデバイス6のCPU53に設定可能な条件を問い合わせ、その回答を得る。ステップS103において移動管理プログラム134は、曲データベース中に登録されているフォーマットの条件のうち、相手先の機器に設定可能な条件をステップS102で調べた条件に基づいて決定する。

【0230】ステップS104において、移動管理プログラム134は、設定可能な条件が存在するか否かを判定し、設定可能な条件が存在しない場合には、ステップS105に進み、コンテンツをポータブルデバイス6に移動する処理を禁止する。すなわち、この場合には、曲データベース中に登録されている条件をポータブルデバイス6が守ることができないので、そのようなポータブルデバイス6には、コンテンツを移動することが禁止されるのである。

【0231】ステップS104において設定可能な条件が存在すると判定された場合、ステップS106に進

み、移動管理プログラム134は、利用条件変換プログラム139に、その条件を相手先の機能フォーマットの条件（例えば、ポータブルデバイス6に転送する際、ヘッダに格納される条件）に変換させる。そして、ステップS107において、移動管理プログラム134は、変換した条件を相手先の機器に設定する。その結果、ポータブルデバイス6は、設定された条件に従って（その条件を守って）、コンテンツを再生することが可能となる。

【0232】次に、図18乃至図20のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、HDD21からポータブルデバイス6にコンテンツをコピーする場合の処理について説明する。この図18乃至図20のステップS111乃至ステップS127の処理は、コピー管理プログラム133により実行され、図12乃至図14のHDD21からポータブルデバイス6へコンテンツを移動させる場合のステップS51乃至ステップS67の処理と同様の処理である。すなわち、この場合においても、曲データベースの改竄がチェックされた後、選択されたコンテンツの再生条件とのチェック処理が行われる。さらに、ポータブルデバイス6と、パーソナルコンピュータ1との間の相互認証処理の後、コンテンツが、パーソナルコンピュータ1のHDD21からポータブルデバイス6のフラッシュメモリ61に転送され、保存される。その後、ステップS128において、コピー管理プログラム133は、曲データベースのコピー回数カウンタを1だけインクリメントする。そして、ステップS129において、コピー管理プログラム133は、CPU32に、曲データベース全体のハッシュ値を計算させ、その値を不揮発性メモリ34に保存させる。

【0233】次に、図21のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、ポータブルデバイス6からHDD21にコンテンツを移動する処理およびチェックインの処理について説明する。

【0234】始めに、コンテンツの移動の処理について説明する。ステップS161において、移動管理プログラム134は、ポータブルデバイス6のCPU53に対してフラッシュメモリ61に記憶されているコンテンツの情報の読み出しを要求する。CPU53は、この要求に対応して、フラッシュメモリ61に記憶されているコンテンツの情報をパーソナルコンピュータ1に送信する。移動管理プログラム134は、この情報に基づいて、ディスプレイ20に、フラッシュメモリ61に記憶されているコンテンツを選択するためのGUIを表示させる。使用者は、キーボード18またはマウス19を操作して、そのGUIに基づいて、ポータブルデバイス6からHDD21（コンテンツデータベース114）に移動させるコンテンツを指定する。

【0235】ステップS162において、移動管理プログラム134は、認証プログラム141に、CPU53との間において、相互認証処理を実行させ、通信用鍵を共有させる。この処理は、図12のステップS56における場合と同様の処理である。

【0236】次に、ステップS163において、CPU53は、フラッシュメモリ61に記憶されている暗号化されている選択されたコンテンツを読み出し、パーソナルコンピュータ1に転送する。移動管理プログラム134は、ステップS164において、ポータブルデバイス6から転送されてきたコンテンツを、1つのファイルとしてファイル名を付けて、コンテンツデータベース114 (HDD21) に保存する。この保存は、例えば、1つのファイルの一部として、ファイル名の位置情報 (例えば、先頭からのバイト数) を与えて行うようにすることもできる。

【0237】ステップS165において、CPU53は、フラッシュメモリ61に記憶されている選択されたコンテンツの暗号化されている暗号鍵を読み出し、それを自分自身の保存用鍵で復号し、さらに通信用鍵で暗号化した後、パーソナルコンピュータ1に転送する。この暗号鍵は、例えば、図14のステップS67の処理でフラッシュメモリ61に保存されていたものである。

【0238】ステップS166において、移動管理プログラム134は、ポータブルデバイス6から暗号鍵の転送を受けると、復号プログラム142に、それを通信用鍵で復号させ、暗号化プログラム137に、自分自身の保存用鍵で暗号化させる。ステップS167で、移動管理プログラム134は、コンテンツデータベース114に、ステップS164で保存したコンテンツのファイル名、そのコンテンツの情報、使用者がGUIを介して入力した曲名、ステップS166で暗号化した暗号鍵などを、HDD21の曲データベースに登録させる。そして、ステップS168において、移動管理プログラム134は、利用条件管理プログラム140に、その曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させる。

【0239】ステップS169において、移動管理プログラム134は、ポータブルデバイス6に対して暗号鍵が保存されたことを通知し、そのコンテンツの削除を要求する。CPU53は、パーソナルコンピュータ1から、そのコンテンツの削除が要求されてきたとき、ステップS170において、フラッシュメモリ61に記憶されているそのコンテンツを削除する。

【0240】次に、ポータブルデバイス6からパーソナルコンピュータ1にコンテンツをチェックインする処理について説明する。ポータブルデバイス6からパーソナルコンピュータ1にコンテンツをチェックインする処理は、図21のポータブルデバイス6からパーソナルコンピュータ1へコンテンツを移動させる場合と同様の処理

である。すなわち、チェックインの処理は、パーソナルコンピュータ1においてチェックイン/チェックアウト管理プログラム132により実行され、図21のステップS162乃至S166の処理が省略される。また、パーソナルコンピュータ1は、図21のステップS167において、曲データベースに登録されている、チェックインされたコンテンツのチェックアウトできる回数を更新する処理を実行して、ステップS170の処理の後、コンテンツファイルの削除を確認することを除いて、移動の場合の処理と基本的に同様の処理となるので、その処理の詳細の説明は省略する。

【0241】なお、ポータブルデバイス6のフラッシュメモリ61がメモリカードとして着脱可能であるとき、パーソナルコンピュータ1は、チェックインの処理において、図21のステップS162の相互認証の処理を実行する。

【0242】また、前述のように、所定のパーソナルコンピュータからチェックアウトされたコンテンツが、該パーソナルコンピュータにのみチェックインできるようになっており、チェックイン処理の前処理として、選択されたコンテンツが、チェックインを行うPCからチェックアウトされたかを判断し、該PCからチェックアウトされたものではないと判断されたらば、チェックインを行わないように処理するステップが存在する。例えば、図5のフィールド213の×がついたコンテンツをチェックインしようとした場合がそれにあたる。

【0243】次に、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、ポータブルデバイス6からHDD21へコンテンツをコピーする場合の処理について、図22のフローチャートを参照して説明する。この図22に示すステップS181乃至ステップS188の処理は、図21のポータブルデバイス6からHDD21へコンテンツを移動させる場合の処理におけるステップS161乃至ステップS168の処理と同様の処理である。すなわち、コピー処理の場合は、コピー管理プログラム133により実行され、図21のステップS169、S170の処理が省略される点を除いて、移動の場合の処理と基本的に同様の処理となるので、その説明は省略する。

【0244】次に、図23のフローチャートを参照して、EMDサーバ4およびコンテンツ管理プログラム111を実行するCPU11による、EMDサーバ4から転送を受けたコンテンツをHDD21にコピーする処理について説明する。ステップS201において、購入用プログラム144は、図5に示すボタン202がクリックされて、使用者からEMDサーバ4へのアクセスが指令されたとき、通信部25を制御し、ネットワーク2を介してEMDサーバ4にアクセスさせる。EMDサーバ4は、このアクセスに対応して、自分自身が保持しているコンテンツの曲番号、曲名、各情報などの情報を、ネットワーク2を

介してパーソナルコンピュータ1に転送する。購入用プログラム144は、通信部25を介して、この情報を取得したとき、表示操作指示プログラム112に、それをインタフェース17を介してディスプレイ20に表示させる。使用者は、ディスプレイ20に表示されたGUIを利用して、ステップS202において、コピーを希望するコンテンツを指定する。この指定情報は、ネットワーク2を介してEMDサーバ4に転送される。ステップS203において、購入用プログラム144は、EMDサーバ4との間において、ネットワーク2を介して相互認証処理を実行し、通信用鍵を共有する。

【0245】パーソナルコンピュータ1とEMDサーバ4の間で行われる相互認証処理は、例えば、ISO 9798-3で規定される公開鍵と秘密鍵を用いて行うようにすることができる。この場合、パーソナルコンピュータ1は、自分自身の秘密鍵とEMDサーバ4の公開鍵を予め有しており、EMDサーバ4は、自分自身の秘密鍵を有し、相互認証処理が行われる。パーソナルコンピュータ1の公開鍵は、EMDサーバ4から転送したり、あるいはパーソナルコンピュータ1に予め配布されている証明書(certificate)をパーソナルコンピュータ1からEMDサーバ4に転送し、その証明書をEMDサーバ4が確認し、公開鍵を得るようにしてもよい。さらに、ステップS204において、購入用プログラム144は、EMDサーバ4との間において課金に関する処理を実行する。この課金の処理の詳細は、図24のフローチャートを参照して後述する。

【0246】次に、ステップS205において、EMDサーバ4は、パーソナルコンピュータ1に対して、ステップS202で指定された、暗号化されているコンテンツをネットワーク2を介してパーソナルコンピュータ1に転送する。このとき、時刻情報も適宜転送される。ステップS206において、購入用プログラム144は、コンテンツデータベース114に、転送を受けたコンテンツにファイル名を付けてHDD21に1つのコンテンツファイル161として保存させる。ステップS207において、EMDサーバ4は、さらに、そのコンテンツの暗号鍵をステップS203でパーソナルコンピュータ1と共有した通信用鍵を用いて暗号化し、パーソナルコンピュータ1へ転送する。

【0247】購入用プログラム144は、ステップS208において、復号プログラム142に、EMDサーバ4より転送を受けた暗号鍵を単独で、またはアダプタ26のCPU32と共同して通信用鍵を用いて復号させ、暗号化プログラム137に、復号して得られた暗号鍵を自分自身の保存用鍵で暗号化させる。ステップS209において、購入用プログラム144は、コンテンツデータベース114に、そのコンテンツのファイル名、コンテンツの情報、使用者が入力した曲名、暗号化された暗号鍵を組にして、HDD21の曲データベースに登録させる。

さらに、ステップS210において、購入用プログラム144は、その曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に保存させる。

【0248】なお、ステップS205においてEMDサーバ4は、コンテンツとともに、時刻データをパーソナルコンピュータ1に送信する。この時刻データは、パーソナルコンピュータ1からアダプタ26に転送される。アダプタ26のCPU32は、パーソナルコンピュータ1より転送されてきた時刻データを受信すると、ステップS211において、RTC35の時刻を修正させる。このようにして、相互認証の結果、正しい装置と認識された外部の装置から得られた時刻情報に基づいて、アダプタ26のRTC35の時刻情報を修正するようにしたので、アダプタ26を常に正しい時刻情報を保持することが可能となる。

【0249】次に、図24のフローチャートを参照して、EMDサーバ4およびコンテンツ管理プログラム111を実行するCPU11による、図23のステップS204における課金に関する処理の詳細について説明する。ステップS221において、購入用プログラム144は、ステップS201でEMDサーバ4から伝送されてきた価格情報の中から、ステップS202で指定された選択されたコンテンツの価格情報を読み取り、これをHDD21上の課金ログに書き込む。図25は、このような課金ログの例を表している。この例においては、使用者は、アイテム1乃至アイテム3を、EMDサーバ4からコピーしており、アイテム1とアイテム2の領域は50円とされ、アイテム3の料金は60円とされている。その時点における課金ログのハッシュ値も、CPU32により計算され、不揮発性メモリ34に登録されている。

【0250】次に、ステップS222において、購入用プログラム144は、ステップS221で書き込んだ課金ログをHDD21から読み出し、これをネットワーク2を介してEMDサーバ4に転送する。EMDサーバ4は、ステップS223において、パーソナルコンピュータ1から転送を受けた課金ログに基づく課金計算処理を実行する。すなわち、EMDサーバ4は、内蔵するデータベースに、パーソナルコンピュータ1の使用者から伝送されてきた課金ログを追加更新する。そして、ステップS224において、EMDサーバ4は、その課金ログについて直ちに決裁するか否かを判定し、直ちに決裁する場合には、ステップS225に進み、EMDサーバ4は、決裁に必要な商品名、金額などを決裁サーバ(図示せず)に転送する。そして、ステップS226において、決裁サーバは、パーソナルコンピュータ1の使用者に対する決裁処理を実行する。ステップS224において、決裁は直ちには行われないと判定された場合、ステップS225とS226の処理はスキップされる。すなわち、この処理は、例えば、月に1回など、定期的にその後実行される。

【0251】次に、図26と図27のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、音声入出力インタフェース24のIEC60958端子24aから入力された、図示せぬCDプレーヤなどからの再生されたコンテンツを、HDD21にコピーする場合の処理について説明する。ステップS241において、使用者は、CDプレーヤのIEC60958出力端子を、パーソナルコンピュータ1の音声入出力インタフェース24のIEC60958端子24aに接続する。ステップS242において、使用者は、キーボード18またはマウス19を操作し、CDプレーヤからコピーするコンテンツの曲名（または、コンテンツに対応する番号）を入力する。そして、ステップS243において使用者は、CDプレーヤのボタンを操作し、CDプレーヤの再生を開始させる。CDプレーヤとパーソナルコンピュータ1との間に制御信号を送受する線が接続されている場合には、パーソナルコンピュータ1のキーボード18またはマウス19を介して再生開始指令を入力することで、CDプレーヤにCDの再生を開始させることも可能である。

【0252】CDプレーヤにおいて、CDの再生が開始されると、ステップS244において、CDプレーヤから出力されたコンテンツが、IEC60958端子24aを介してパーソナルコンピュータ1に転送されてくる。ステップS245において、コピー管理プログラム133は、IEC60958端子24aを介して入力されてくるデータから、SCMS (Serial Copy Management System) データを読み取る。このSCMSデータには、コピー禁止、コピー1回限り可能、コピーフリーなどのコピー情報が含まれている。そこで、ステップS246において、CPU11は、SCMSデータがコピー禁止を表しているか否かを判定し、コピー禁止を表している場合には、ステップS247に進み、コピー管理プログラム133は、表示操作指示プログラム112に、例えば、「コピーが禁止されています」といったメッセージをディスプレイ20に表示させ、コピー処理を終了する。すなわち、この場合には、HDD21へのコピーが禁止される。

【0253】コピー管理プログラム133は、ステップS246において、ステップS245で読み取ったSCMS情報がコピー禁止を表していないと判定した場合、ステップS248に進み、ウォーターマークコードを読み出し、そのウォーターマークがコピー禁止を表しているか否かをステップS249において判定する。ウォーターマークコードがコピー禁止を表している場合には、ステップS247に進み、上述した場合と同様に、所定のメッセージが表示され、コピー処理が終了される。

【0254】ステップS249において、ウォーターマークがコピー禁止を表していないと判定された場合、ステップS250に進み、期限データベースチェック処理が行われる。期限データベースチェックの結果、選択されたコンテンツが既に登録されていれば、ステップS25

1、S252の処理で、処理が終了される。この処理は、図7のステップS13、S14の処理と同様の処理である。

【0255】選択されたコンテンツがまだHDD21に登録されていないコンテンツであれば、ステップS253乃至S258で、その登録処理が実行される。このステップS253乃至ステップS258の処理は、ステップS257において、IEC60958端子24aから供給されてくるSCMS情報も曲データベースに登録される点を除き、図7のステップS19乃至ステップS24の処理と同様の処理であるので、その説明は省略する。

【0256】次に、図28と図29のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、コンテンツをHDD21からIEC60958端子24aに出力（再生）する場合の処理について説明する。ステップS271乃至ステップS273において、図18のステップS111乃至S113における場合と同様に、曲データベース全体のハッシュ値が計算され、前回保存しておいたハッシュ値と一致するか否かが判定され、曲データベースの改竄のチェック処理が行われる。曲データベースの改竄が行われていないと判定された場合、ステップS274に進み、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、HDD21の曲データベースにアクセスさせ、そこに登録されている曲の情報を読み出させ、ディスプレイ20に表示させる。使用者は、その表示を見て、キーボード18またはマウス19を適宜操作して、再生出力するコンテンツを選択する。ステップS275において、表示操作指示プログラム112は、選択されたコンテンツの再生条件等のチェック処理を実行する。この再生条件等のチェック処理の詳細は、図30のフローチャートを参照して後述する。

【0257】次に、ステップS276において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、ステップS274において選択されたコンテンツの暗号鍵を曲データベースから読み出させ、復号プログラム142に保存用鍵で復号させる。ステップS277において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、選択されたコンテンツのSCMS情報を曲データベースから読み出させ、IEC60958端子24aから出力するSCMS情報を、SCMSシステムの規則に従って決定する。例えば、再生回数に制限があるような場合、再生回数は1だけインクリメントされ、新たなSCMS情報とされる。ステップS278において、表示操作指示プログラム112はさらに、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、選択されたコンテンツのISRCを曲データベースから読み出させる。

【0258】次に、ステップS279において、表示操

作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、曲データベースから選択されたコンテンツファイル名を読み出させ、そのファイル名を基に、そのコンテンツをHDD21から読み出させる。表示操作指示プログラム112はさらに、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、そのコンテンツに対応する暗号鍵を曲データベースから読み出させ、復号プログラム142に、保存用鍵で復号させ、復号した暗号鍵を用いて、暗号化されているコンテンツを復号する。圧縮／伸張プログラム138は、さらに、そのコンテンツの圧縮符号を復号（伸張）する。ステップS280において、表示操作指示プログラム112は、ドライバ117に、ステップS279で、復号したデジタルデータであるコンテンツを、ステップS277で決定したSCMS情報、並びにステップS278で読み出したISRC情報とともに、IEC60958の規定に従って、IEC60958端子24aから出力させる。さらにまた、表示操作指示プログラム112は、例えば、図示せぬリアルプレーヤ（商標）などのプログラムを動作させ、デジタルデータであるコンテンツをアナログ化させ、音声入出力インタフェース24のアナログ出力端子から出力させる。

【0259】ステップS281において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、曲データベース中の再生回数カウンタの値を1だけインクリメントさせる。そして、ステップS282において、選択されたコンテンツに再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS283に進み、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、対応する料金を課金ログに書き込ませ、ステップS284において、表示操作指示プログラム112は、利用条件管理プログラム140に、曲データベース全体のハッシュ値をCPU32に計算させ、不揮発性メモリ34に記憶させる。ステップS282において、選択されたコンテンツに再生時課金条件が付加されていないと判定された場合、ステップS283とステップS284の処理はスキップされる。

【0260】次に、図30のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11による、図28のステップS275の再生条件等のチェック処理の詳細について説明する。ステップS301において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介して、コンテンツデータベース114に、曲データベースの各種条件を読み出させる。ステップS302において利用条件管理プログラム140は、読み出した条件のうち、再生回数が制限回数を過ぎているか否かを判定し、過ぎている場合には、ステップS303に進み、コンテンツ管理プログラム11

1を介して、コンテンツデータベース114に、選択されたコンテンツをHDD21から削除させるとともに、曲データベースから選択されたコンテンツの情報を削除させる。ステップS304において、表示操作指示プログラム112はさらに、利用条件管理プログラム140に、曲データベースの新たなハッシュ値をCPU32に計算させ、そのハッシュ値を不揮発性メモリ34に保存させる。この場合、再生出力は禁止される。

【0261】ステップS302において、再生回数が制限回数を過ぎていないと判定された場合、ステップS305に進み、利用条件管理プログラム1402は、再生終了日時が現在日時を過ぎているか否かを判定する。再生終了日時が現在日時を過ぎている場合には、上述した場合と同様にステップS303において、選択されたコンテンツをHDD21から削除させるとともに、曲データベースからも削除させる。そして、ステップS304において、新たな曲データベースのハッシュ値が計算され、保存される。この場合にも、再生出力は禁止される。

【0262】ステップS305において、再生終了日時が現在日時を過ぎていると判定された場合は、ステップS306に進み、CPU32は、その選択されたコンテンツに対して再生時課金条件が付加されているか否かを判定する。再生時課金条件が付加されている場合には、ステップS307に進み、表示操作指示プログラム112は、再生時課金条件が付加されている旨のメッセージと料金を、ディスプレイ20に表示させる。ステップS306において、再生時課金条件が付加されていないと判定された場合、ステップS307の処理はスキップされる。

【0263】次に、図31と図32のフローチャートを参照して、コンテンツ管理プログラム111を実行するCPU11およびメインプログラムを実行するCPU53による、HDD21からポータブルデバイス6経由でコンテンツを出力（再生）する場合の処理について説明する。ステップS321乃至ステップS325において、曲データベースの改竄チェックと選択されたコンテンツの指定、並びに選択されたコンテンツの再生条件等のチェック処理が行われる。その処理は、図28のステップS271乃至ステップS275の処理と同様の処理であるので、その説明は省略する。

【0264】ステップS326において、ポータブルデバイス6とパーソナルコンピュータ1の間で相互認証処理が実行され、相互の間で、通信用鍵が共有される。ステップS327において、表示操作指示プログラム112は、ポータブルデバイス6に対して、これから送る暗号化されているコンテンツを再生するように命令する。ステップS328において、表示操作指示プログラム112は、ステップS324で、コンテンツ管理プログラム111を介してコンテンツデータベース114に、指

10

20

30

40

50

定された選択されたコンテンツのファイル名を曲データベースから読み出させ、そのファイル名のコンテンツをHDD 21から読み出させる。表示操作指示プログラム112は、ステップS329において、コンテンツ管理プログラム111に、コンテンツの圧縮符号化方式、暗号化方式、フォーマットなどをポータブルデバイス6の方式のものに変換する処理を実行させる。そして、ステップS330において、表示操作指示プログラム112は、暗号化プログラム137に、ステップS329において変換したコンテンツを通信用鍵で暗号化させ、ポータブルデバイス6に転送する。

【0265】ステップS331において、ポータブルデバイス6のCPU53は、ステップS327において、パーソナルコンピュータ1から転送されてきた命令に対応して、転送を受けた各データを通信用鍵で復号し、再生出力する。ステップS332において、表示操作指示プログラム112は、コンテンツ管理プログラム111を介してコンテンツデータベース114に、曲データベースの再生回数カウントを1だけインクリメントさせる。さらに、ステップS333において、表示操作指示プログラム112は、選択されたコンテンツに再生時課金条件が付加されているか否かを判定し、付加されている場合には、ステップS334において、コンテンツ管理プログラム111を介してコンテンツデータベース114に、その料金を課金ログに書き込ませ、ステップS335において、CPU52に、曲データベース全体のハッシュ値を新たに計算させ、保存させる。選択されたコンテンツに再生時課金条件が付加されていない場合には、ステップS334、ステップS335の処理はスキップされる。

【0266】本発明においては、コンテンツが不正に複製されるのを防止するために、各種の工夫が凝らされている。例えば、CPU11を動作させるプログラムは、その実行順序が毎回変化するような、いわゆるタンパーレジスタントソフトウェアとされている。

【0267】さらに、上述したように、CPU11の機能の一部は、ハードウェアとしてのアダプタ26に分担され、両者が共働して各種の処理を実行するようになっている。これにより、より安全性を高めることが可能となっている。

【0268】例えば、上述したように、曲データベースのハッシュ値は、曲データベース自体に保存されるのではなく、アダプタ26の不揮発性メモリ34に保存される。すなわち、図8のステップS32、S33などの前回保存しておいたハッシュ値との比較処理において、比較対象とされる過去のハッシュ値は、不揮発性メモリ34に記憶されているものとされる。これにより、例えば、他の記録媒体にコピーまたは移動させる前に、HDD 21に保存されているコンテンツを含む記録内容の全てをバックアップしておき、HDD 21から、そこに保存さ

れているコンテンツを他の記録媒体にコピーまたは移動した後、HDD 21にバックアップしておいた記録内容に含まれるコンテンツを再びリストアするようにすることで、利用条件を無視して、実質的に際限なく、コピーまたは移動ができてしまうようなことが防止される。

【0269】例えば、図33に示すように、HDD 21にコンテンツA、Bが保存されている場合、不揮発性メモリ34には、コンテンツAとコンテンツBの情報に対応するハッシュ値が保存されている。この状態において、HDD 21のコンテンツA、Bを含む記録データの一部または全部を他の記録媒体271にバックアップしたとする。その後、HDD 21に保存されているコンテンツAとコンテンツBのうち、コンテンツAを他の記録媒体272に移動させた場合、その時点において、HDD 21に記録されているコンテンツは、コンテンツBだけとなるので、不揮発性メモリ34のハッシュ値も、コンテンツBに対応するハッシュ値に変更される。

【0270】従って、その後、記録媒体271にバックアップしておいたHDD 21のコンテンツA、Bを含む記録データの一部または全部をHDD 21にリストアして、HDD 21に、再びコンテンツAとコンテンツBを保存させたとしても、不揮発性メモリ34には、コンテンツBの情報から演算されたハッシュ値が記憶されており、コンテンツAとコンテンツBの情報から演算されたハッシュ値は記憶されていない。これにより、その時点において、HDD 21に記憶されているコンテンツAとコンテンツBに基づくハッシュ値が、不揮発性メモリ34に記憶されている過去のハッシュ値と一致しないことになり、曲データベースが改竄されたことが検出される。その結果、以後、HDD 21に保存されているコンテンツAとコンテンツBの利用が制限されてしまうことになる。

【0271】さらに、上述したように、アダプタ26は、RTC35を内蔵しており、このRTC35の値は、正しい認証結果が得られた他の装置（例えば、EMDサーバ4）から転送されてきた時刻データに基づいて、その時刻情報を修正する。そして、現在日時としては、パーソナルコンピュータ1が管理するものではなく、RTC35が出力するものが利用される。従って、使用者が、パーソナルコンピュータ1の現在時刻を故意に過去の時刻に修正し、再生条件としての再生終了日時の判定を免れるようなことができなくなる。

【0272】また、アダプタ26は、暗号化されて転送されてきたプログラムをROM36に予め記憶されているプログラムに従って復号し、実行するように構成することで、より安全性が高められている。次に、この点について、図34のフローチャートを参照して説明する。

【0273】すなわち、パーソナルコンピュータ1は、アダプタ26に対して、所定の処理を実行させたいとき、ステップS351において、アダプタ26に実行させるべきプログラムをRAM13に予め記憶されている暗

号鍵を用いて暗号化してアダプタ 26 に転送する。アダプタ 26 の ROM 36 には、パーソナルコンピュータ 1 から転送されてきた、暗号化されているプログラムを復号し、実行するためのプログラムが予め記憶されている。CPU 32 は、この ROM 36 に記憶されているプログラムに従って、パーソナルコンピュータ 1 から転送されてきた暗号化されているプログラムをステップ S 352 において復号する。そして、ステップ S 313 において、CPU 32 は、復号したプログラムを RAM 33 に展開し、ステップ S 354 において、そのプログラムを実行する。

【0274】例えば、上述したように、パーソナルコンピュータ 1 の CPU 11 は、HDD 21 の曲データベースのハッシュ値をアダプタ 26 に計算させるとき、曲データベースのデータを暗号鍵で暗号化してアダプタ 26 の CPU 32 に転送する。CPU 32 は、転送されてきた曲データベースのデータに対してハッシュ関数を適応し、ハッシュ値を計算する。そして、計算されたハッシュ値を不揮発性メモリ 34 に記憶させる。あるいは、そのハッシュ値を、CPU 32 は、予め記憶されている過去のハッシュ値と比較し、比較結果をパーソナルコンピュータ 1 の CPU 11 に転送する。

【0275】図 35 は、アダプタ 26 の内部のより具体的な構成を表している。アダプタ 26 は、半導体 IC として形成される。アダプタ 26 は、図 2 に示したインタフェース 31、CPU 32、RAM 33、不揮発性メモリ 34、RTC 35、ROM 36 以外に、RAM 33 に対する書き込みと読み出しを制御する RAM コントローラ 301、並びに論理回路 302 を有している。論理回路 302 は、例えば、暗号化されているコンテンツを解読した後、解読したデータをアダプタ 26 から直接出力するような場合の処理のために用いられる。

【0276】これらのインタフェース 31 乃至 ROM 36、RAM コントローラ 301、並びに論理回路 302 は、半導体 IC 内に一体的に組み込まれ、外部からは分解できないように構成されている。

【0277】水晶振動子 311 は、アダプタ 26 が各種の処理を実行する上において、基準となるクロックを生成するとき用いられる。発振回路 312 は、RTC 35 を動作させるための発振回路である。バッテリー 313 は、発振回路 312、不揮発性メモリ 34、および RTC 35 に対してバックアップ用の電力を供給している。アダプタ 26 のその他の回路には、パーソナルコンピュータ 1 の電源供給回路 321 からの電力が供給されている。

【0278】不揮発性メモリ 34 は、書き込み消去可能な ROM で構成することも可能であるが、バッテリー 313 からのバックアップ電源でバックアップされる RAM で構成する場合には、例えば、図 36 に示すように、不揮発性メモリ 34 の上に保護アルミニウム層 351 を形成し、さらに、その保護アルミニウム層 351 と同一平面上となるように、不揮発性メモリ 34 にバッテリー 313

からの電力を供給する電源パターン 352 を形成することができる。このようにすると、例えば、不揮発性メモリ 34 を改竄すべく、保護アルミニウム層 351 を削除しようとする、同一平面上の電源パターン 352 も削除されてしまい、不揮発性メモリ 34 に対する電力の供給が断たれ、内部に記憶されているデータが消去されてしまうことになる。このように構成することで、タンパーレジスト性をより高めることができる。

【0279】さらに、図 37 に示すように、不揮発性メモリ 34 に対するデータの書き込みまたは読み出しのための配線 401-1 乃至 401-3 は、対応する位置で、上下（深さ）方向に重なりあうように形成されている。これにより、より下層の配線 401-3 からデータを読み出すためには、上方の配線 401-1、401-2 を除去しなければならない、複数の配線 401-1、401-2、401-3 から同時にデータを読み取ることができなくなる。

【0280】さらにまた、不揮発性メモリ 34 は、配線 401-1 乃至 401-3 を冗長に形成するようにすることができる。例えば、不揮発性メモリ 34 内部に形成される配線 401-1 乃至 401-3 が不揮発性メモリ 34 を構成するトランジスタなどの素子を結合するとき、その経路は、例え、直線的に結合が可能であっても、直線的には形成されず、所定の長さとなるように形成される。このようにすることで、配線 401-1 乃至 401-3 の長さは、本来必要な長さ以上の長さとなり、配線に必要な最短の長さの場合に比較して大きな寄生容量を有することとなる。

【0281】不揮発性メモリ 34 からデータを読み出すために設計されている専用の回路（半導体 IC としてのアダプタ 26 に内蔵されている）は、その寄生容量にマッチングしたインピーダンスを設定することで、不揮発性メモリ 34 が記憶しているデータを正常に読み出すことができる。しかしながら、不揮発性メモリ 34 に記憶されているデータを読み出すべく、プローブを配線 401-1 乃至 401-3 に接続させると、その寄生容量とプローブによる合成の容量が影響して、データを正常に読み出すことが困難になる。

【0282】以上においては、記録媒体として、ポータブルデバイス 6 を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。

【0283】また、コンテンツは、曲のデータまたは音声データなどの楽音データ以外に、画像データ、その他のデータとすることもできる。

【0284】以上のように、本発明によれば、次のような効果を奏することができる。

【0285】（1） HDD 21 に暗号化してデータを記録するとともに、暗号鍵も保存用鍵で暗号化した上で HDD 21 に記録するようにしたので、HDD 21 に記録されて

いるコンテンツをコピーしても、これを復号することができないので、複製が大量に配布されることを防止することができる。

【0286】(2) 所定の曲を1回コピーしたとき、一定時間(上記例の場合、48時間)の間、その曲をコピーすることができないようするために、その曲と録音日時を曲データベース上に登録するようにしたので、そのコピー回数を制限することができ、複製を大量に配布することを防止することができる。

【0287】さらにデータベースを更新する度に、データのハッシュ値を計算し保存するようにしたので、データベースの改竄を防止することが容易となる。

【0288】(3) 外部の装置にコンテンツを渡したら、HDD21上のコンテンツを消去するようにしたので、HDD21内に元のデジタルデータであるコンテンツが残らず、その複製を大量に配布することが防止される。

【0289】(4) HDD21内に曲データベースを設け、全体のハッシュ値を毎回チェックするようにしたので、HDD21の内容をムーブの直前にバックアップし、ムーブ直後にバックアップしたデータをHDD21にリストアするようにしたとしても、送り元のデータを確実に消去することが可能となる。

【0290】(5) パーソナルコンピュータ1が外部の機器にデータを渡すとき、その前に相互認証処理を行うようにしたので、不正な機器にデータを渡してしまうようなことが防止される。

【0291】(6) 外部機器から、パーソナルコンピュータ1に対してデータを渡す前に、パーソナルコンピュータ1のソフトウェアが正当なものであるか否かを相互認証により確認するようにしたので、不正なソフトウェアに対してコンテンツを渡してしまうようなことが防止される。

【0292】(7) 曲の同一性の判定にISRCを用い、ISRCが取得できないときは、TOCを用いるようにしたので、ISRCが取得できなくとも、曲の同一性を判定することが可能になる。

【0293】(8) パーソナルコンピュータ1におけるソフトウェア機能のうち、所定の部分をパーソナルコンピュータ1に外付けされるアダプタ26に負担させるようにしたので、パーソナルコンピュータ1のソフトウェアを解析しただけでは、全体としてどのような処理となっているのかが判らないので、ソフトウェアを改竄をして、意図する機能を持たせるようなことが困難となる。

【0294】なお、アダプタ26が実行する処理は、セキュアなプログラムでCPU11が実行するようにしてもよい。この場合において、例えば、同一な値を有する保存用鍵は、保存用鍵が必要になった時点で、コンテンツ管理プログラム111により生成される。同様に、ハッ

シュ値は、コンテンツ管理プログラム111により隠蔽されて保存される。

【0295】また、アダプタ26が実行する処理が、セキュアなプログラムでCPU11により実行されるとき、パーソナルコンピュータ1は、アダプタ26のRTC35が供給する現在時刻に代えて、ネットワーク2に接続されている特定のサーバ(例えば、EMD登録サーバ3)から現在時刻のデータをダウンロードして、その現在時刻を基に、判定の処理を実行する。また、この場合において、パーソナルコンピュータ1は、所定の時間間隔で現在時刻を記憶して、記憶している時刻より以前の時刻が設定されたとき、エラーの表示を行い、時刻の設定を受け付けないようにしてもよい。

【0296】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム格納媒体からインストールされる。

【0297】コンピュータにインストールされ、コンピュータによって実行可能な状態とされるプログラムを格納するプログラム格納媒体は、図2に示すように、磁気ディスク41(フロッピディスクを含む)、光ディスク42(CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む)、光磁気ディスク43(MD(Mini-Disc)を含む)、若しくは半導体メモリ44などよりなるパッケージメディア、または、プログラムが一時的若しくは永続的に格納されるROM12や、HDD21などにより構成される。プログラム格納媒体へのプログラムの格納は、必要に応じて通信部25などのインタフェースを介して、ローカルエリアネットワークまたはインターネットなどのネットワーク2、デジタル衛星放送といった、有線または無線の通信媒体を利用して行われる。

【0298】なお、本明細書において、プログラム格納媒体に格納されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0299】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0300】

【発明の効果】以上の如く、請求項1に記載の情報処理装置、請求項3に記載の情報処理方法、および請求項4に記載のプログラム格納媒体によれば、固定鍵を利用して行われた相互認証処理により、通信用鍵が生成され、

その通信用鍵を、保存用鍵で暗号化して、通信用鍵で暗号化されているデータに対応して、蓄積するようにしたので、蓄積されているデータのコピーが行われたとしても、それを利用することを実質的に防止することができる。とともに、他の装置との間でデータを授受する際にデータがコピーされたとしても、それが利用されるのを防止することができる。

【図面の簡単な説明】

【図 1】本発明に係るコンテンツデータ管理システムの一実施の形態を示す図である。

【図 2】パーソナルコンピュータ 1 の構成を説明する図である。

【図 3】ポータブルデバイス 6 の構成を説明する図である。

【図 4】パーソナルコンピュータ 1 の機能の構成を説明するブロック図である。

【図 5】表示操作指示ウィンドウの例を示す図である。

【図 6】録音プログラム 113 がディスプレイ 20 に表示させるウィンドウの例を説明する図である。

【図 7】コンパクトディスクから HDD 21 にコンテンツをコピーする場合の処理を説明するフローチャートである。

【図 8】図 7 のステップ S12 の期限データベースチェック処理を説明するフローチャートである。

【図 9】期限データベースの例を示す図である。

【図 10】ウォータマークを説明する図である。

【図 11】曲データベースの例を示す図である。

【図 12】HDD 21 からポータブルデバイス 6 へコンテンツを移動する動作を説明するフローチャートである。

【図 13】HDD 21 からポータブルデバイス 6 へコンテンツを移動する動作を説明するフローチャートである。

【図 14】HDD 21 からポータブルデバイス 6 へコンテンツを移動する動作を説明するフローチャートである。

【図 15】図 12 のステップ S55 の選択されたコンテンツの再生条件などのチェック処理を説明するフローチャートである。

【図 16】ポータブルデバイス 6 が管理している再生条件を説明する図である。

【図 17】図 12 のステップ S58 のフォーマット変換処理の詳細を説明するフローチャートである。

【図 18】HDD 21 からポータブルデバイス 6 へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図 19】HDD 21 からポータブルデバイス 6 へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図 20】HDD 21 からポータブルデバイス 6 へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図 21】ポータブルデバイス 6 から HDD 21 へコンテ

ンツを移動する場合の動作を説明するフローチャートである。

【図 22】ポータブルデバイス 6 から HDD 21 へコンテンツをコピーする場合の動作を説明するフローチャートである。

【図 23】EMD サーバ 4 から HDD 21 へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図 24】図 23 のステップ S204 の課金に関する処理の詳細を説明するフローチャートである。

10 【図 25】課金ログを説明する図である。

【図 26】図 2 のパーソナルコンピュータ 1 の IEC60958 端子 24a から HDD 21 へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図 27】図 2 のパーソナルコンピュータ 1 の IEC60958 端子 24a から HDD 21 へコンテンツをコピーする場合の処理を説明するフローチャートである。

【図 28】HDD 21 から IEC60958 端子 24a にコンテンツを出力する場合の動作を説明するフローチャートである。

20 【図 29】HDD 21 から IEC60958 端子 24a にコンテンツを出力する場合の動作を説明するフローチャートである。

【図 30】図 28 のステップ S275 の再生条件などのチェック処理を説明するフローチャートである。

【図 31】HDD 21 からポータブルデバイス 6 経由でコンテンツを出力する場合の動作を説明するフローチャートである。

30 【図 32】HDD 21 からポータブルデバイス 6 経由でコンテンツを出力する場合の動作を説明するフローチャートである。

【図 33】不揮発性メモリ 34 の機能を説明する図である。

【図 34】アダプタ 26 の動作を説明するフローチャートである。

【図 35】アダプタ 26 の内部の構成を示す図である。

【図 36】不揮発性メモリ 34 の内部の構成例を示す図である。

【図 37】不揮発性メモリ 34 の内部の構成例を示す図である。

40 【符号の説明】

1 パーソナルコンピュータ, 2 ネットワーク,
3 EMD登録サーバ, 6-1 乃至 6-3 ポータブルデ
バイス, 11 CPU, 12 ROM, 13 RAM, 2
1 HDD, 24 音声入出力インターフェース, 2
4a IEC60958端子, 26 アダプタ, 32 CP
U, 33 RAM, 34 不揮発性メモリ, 35 RT
C, 36 ROM, 41 磁気ディスク, 42 光デ
ィスク, 43 光磁気ディスク, 44 半導体メモ
リ, 53 CPU, 54 RAM, 55 ROM, 59 D
SP, 61 フラッシュメモリ, 111 コンテンツ

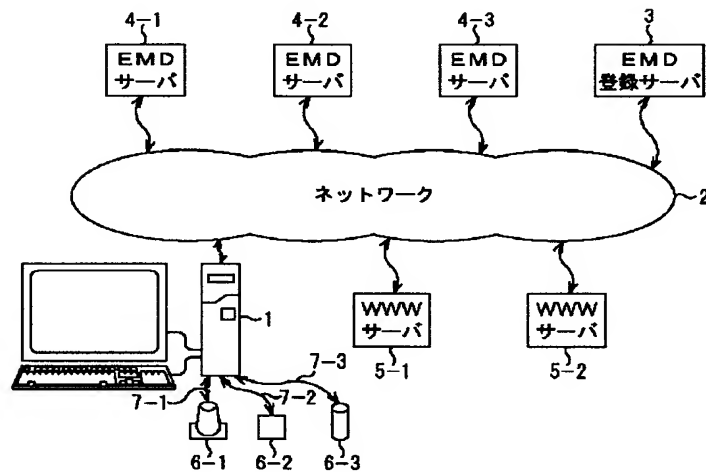
55

管理プログラム, 112 表示操作指示プログラム,
113 録音プログラム, 114 コンテンツデー
タベース, 131 EMD選択プログラム, 132
チェックイン/チェックアウト管理プログラム, 13
3 コピー管理プログラム, 134 移動管理プロ
グラム, 135 暗号方式変換プログラム, 136
圧縮方式変換プログラム, 137 暗号化プロ
グラム, 138 圧縮/伸張プログラム, 139 利用条*

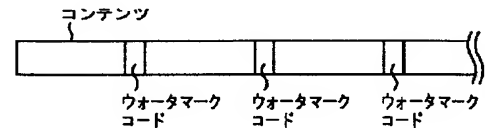
56

*件変換プログラム, 140 利用条件管理プロ
グラム, 141 認証プログラム, 142 復号プロ
グラム, 143 PD用ドライバ, 144 購入用プロ
グラム, 145 購入用プログラム, 181 フィ
タリングデータファイル, 182 表示データフ
イル, 183 画像ファイル, 184 履歴デー
タファイル, 351 保護アルミニウム層, 352
電源パターン, 401-1乃至401-3配線

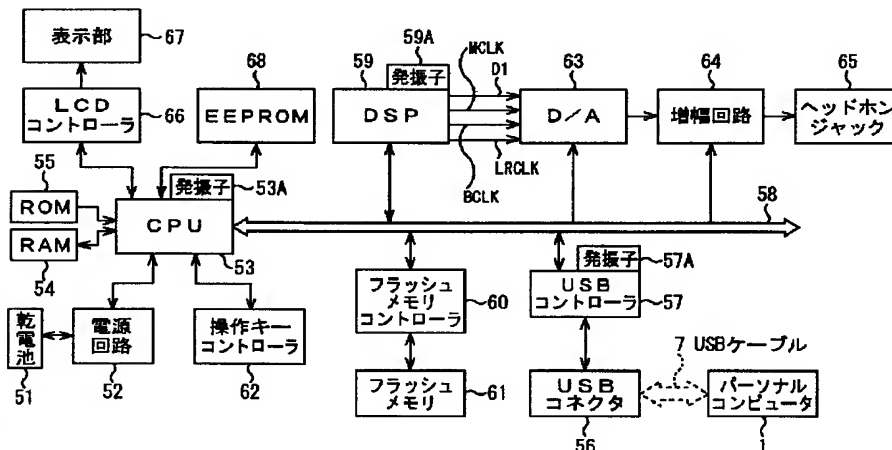
【図1】



【図10】

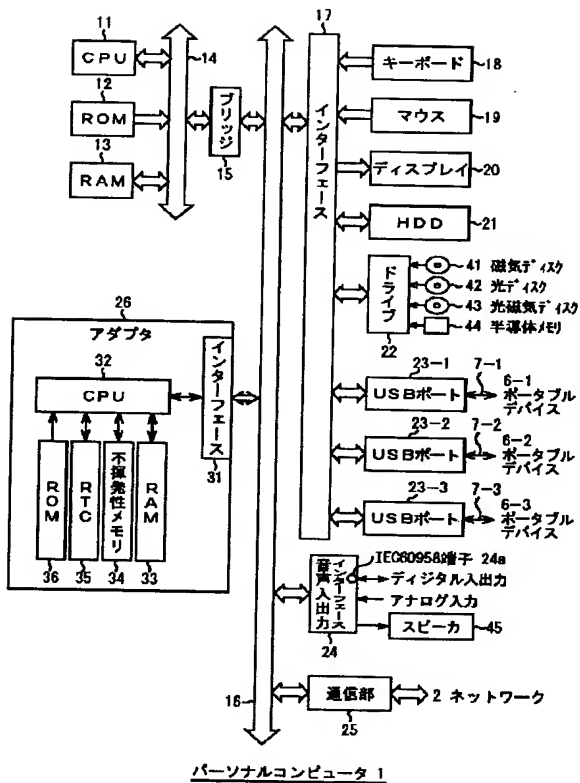


【図3】

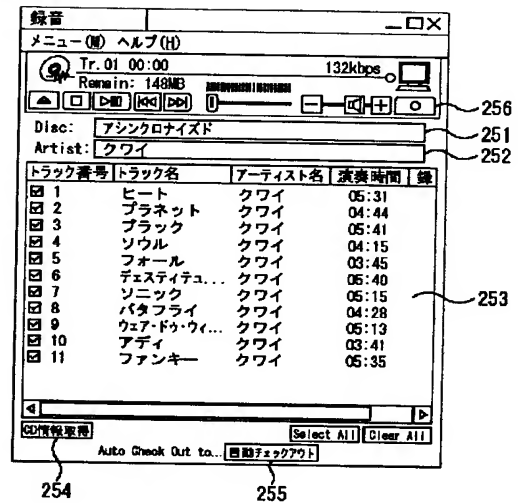


ポータブルデバイス 6

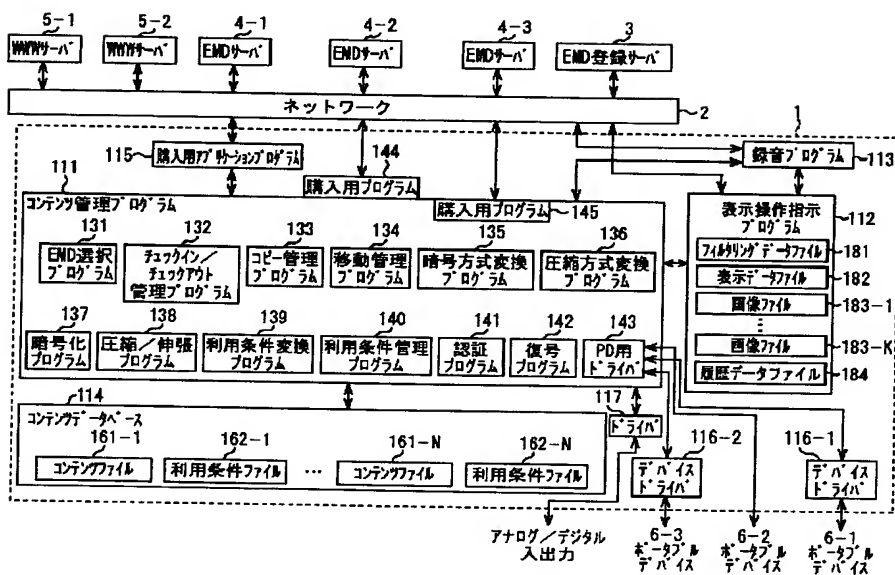
【図2】



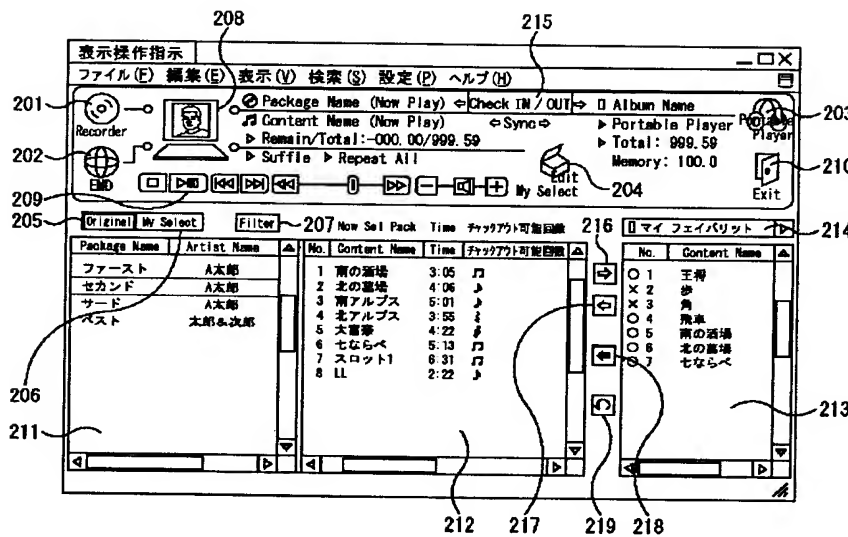
【図6】



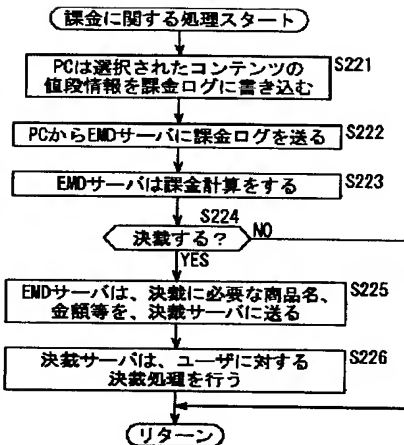
【図4】



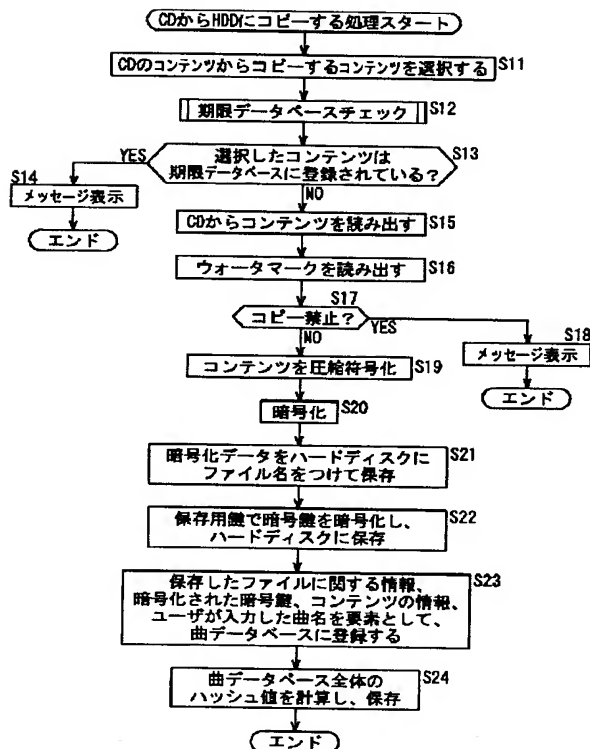
【図5】



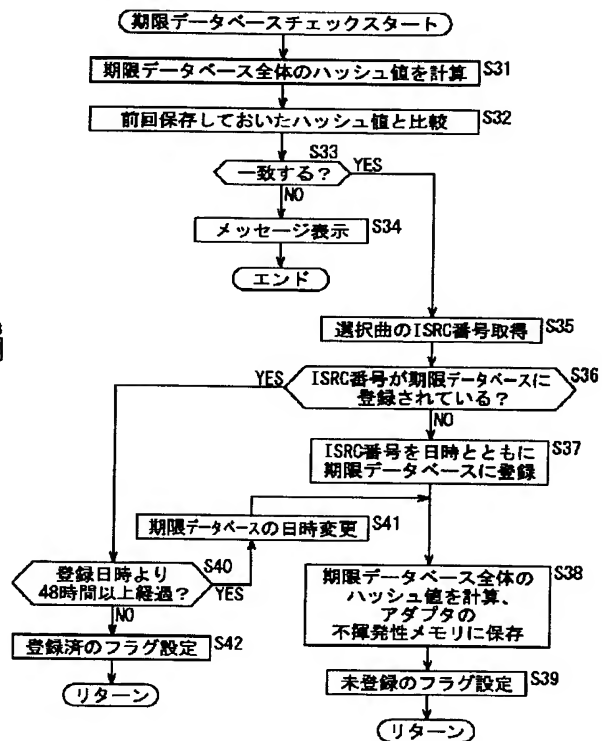
【図24】



【図7】



【図8】



【図9】

期限データベース

	アイテム1	アイテム2	アイテム3	
ISRC	JP-Z90-98-12345	US-Z90-99-12346	JP-Z90-98-12347	
コピー日時	1998.11.23.08:04	2004.03.06.16:09	2004.03.06.16.15	

ハッシュ値	0xf3352e125934
-------	----------------

【図11】

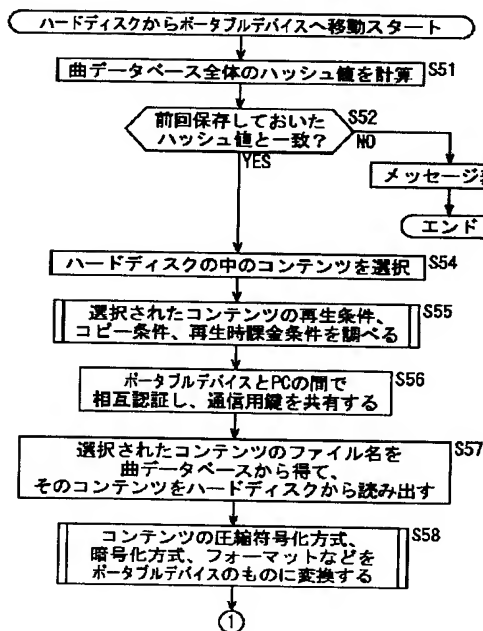
曲データベース

	アイテム1	アイテム2	アイテム3	
ファイル名	xd000110.at2	px92341234.at2	aa0234287034.at2	
暗号化された暗号鍵	0xabababababab	0x9898989898989	0x123456789012	
曲名	春の小川	運命	荒城の月	
長さ	180	190	200	
再生条件:開始日時	-	2001.01.01.00:00	-	
再生条件:終了日時	1999.07.31.23:59	-	-	
再生条件:回数制限	-	20	-	
再生回数カウンタ	-	12	-	
再生時課金条件	-	-	¥5	
コピー条件:回数	2	0	0	
コピー回数カウンタ	1	0	0	
コピー条件:SCMS	0b01	0b10	0b00	

ハッシュ値	0xf9951e566321
-------	----------------

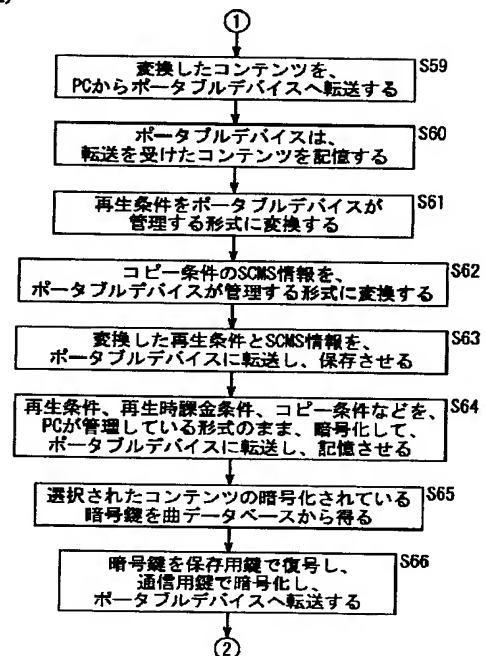
【図12】

(12-1)



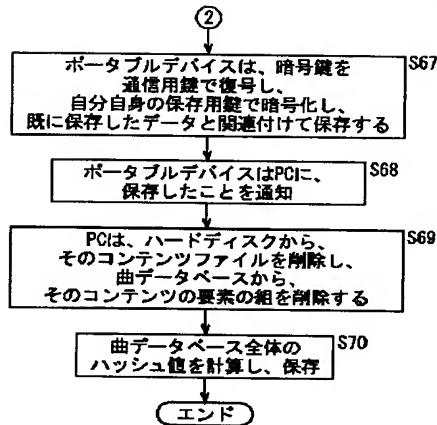
【図13】

(12-2)

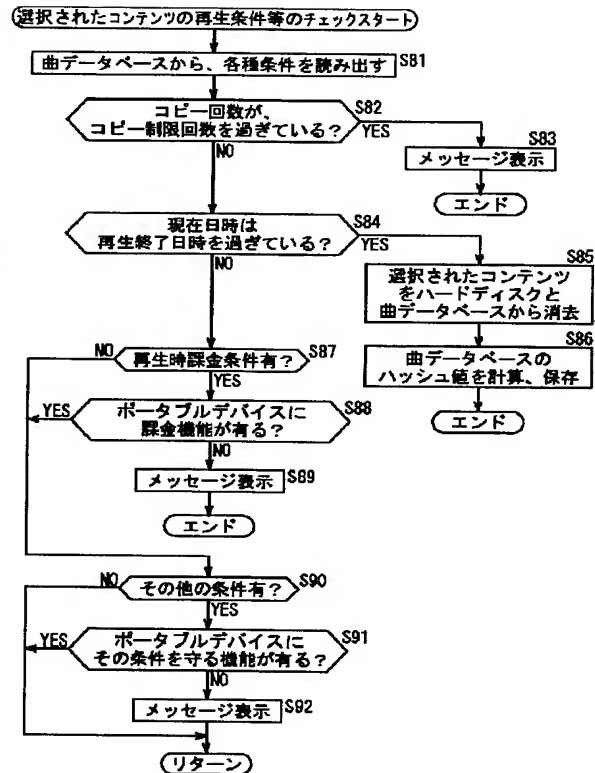


【図14】

(12-3)



【図15】



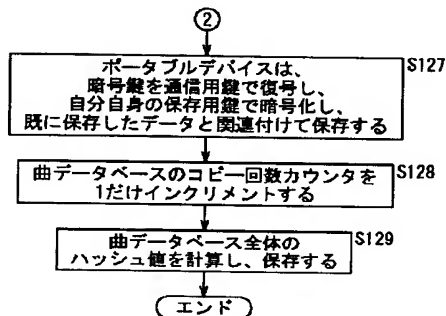
【図16】

ポータブルデバイスが管理している再生条件

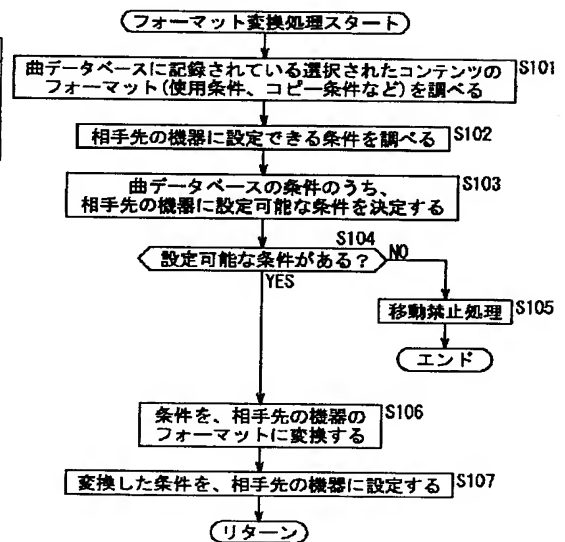
	アイテム1	アイテム2	アイテム3
コンテンツID	00001	00002	00003
再生開始日時	1999.07.31.23:59	1999.07.31.23:59	1999.07.31.23:59
再生終了日時	2001.01.01.00:00	2001.01.01.00:00	2001.01.01.00:00
再生回数	-	15	-

【図20】

(18-3)

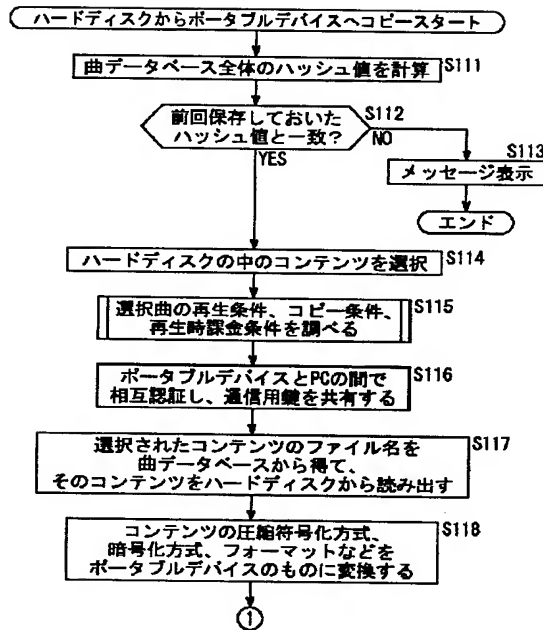


【図17】



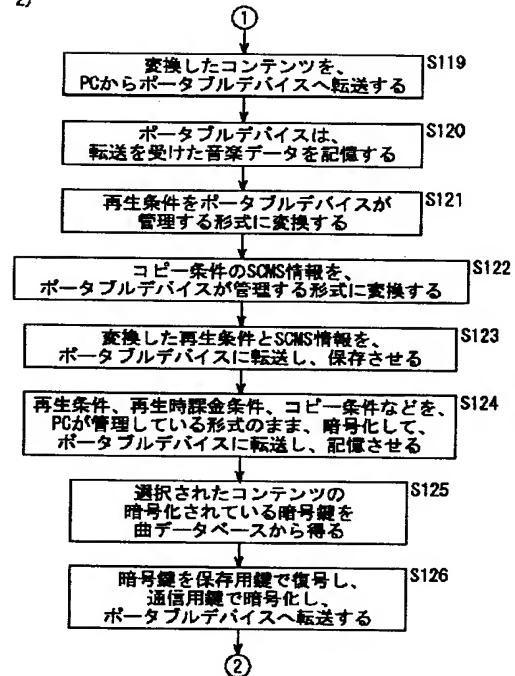
【図18】

(18-1)

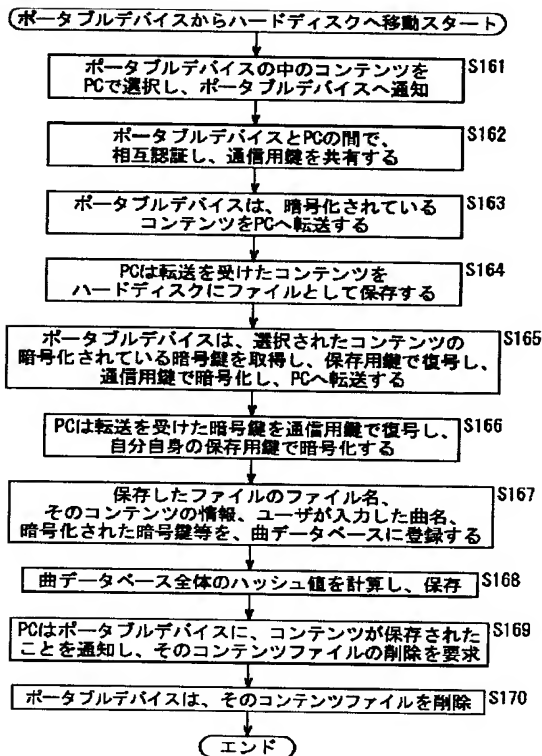


【図19】

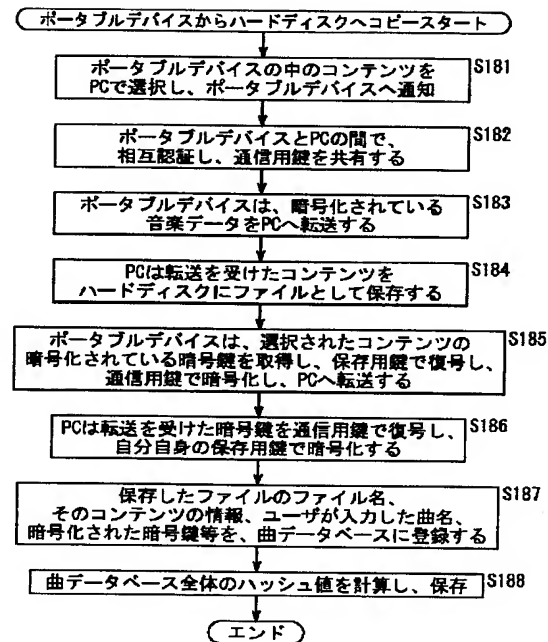
(18-2)



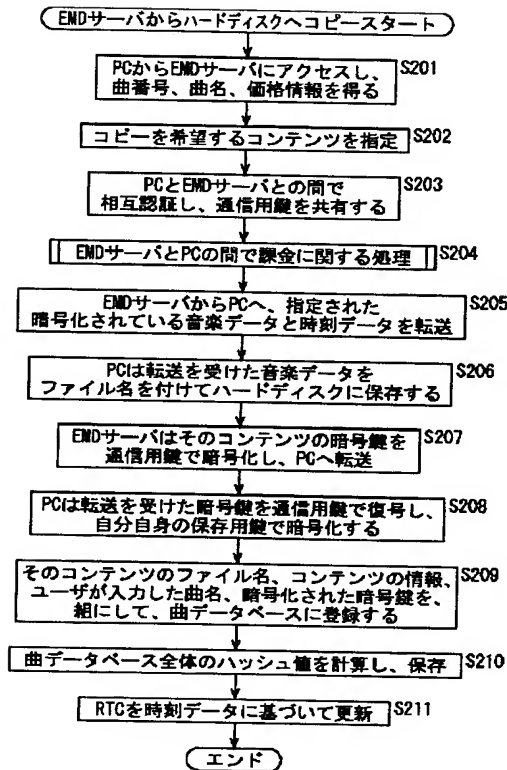
【図21】



【図22】



【図23】

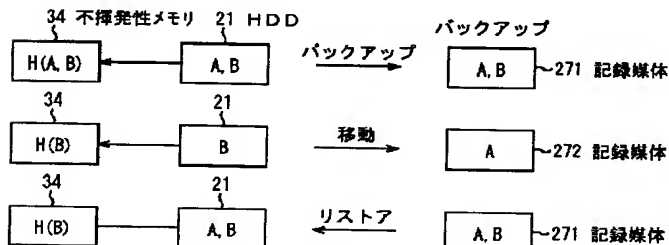


【図25】

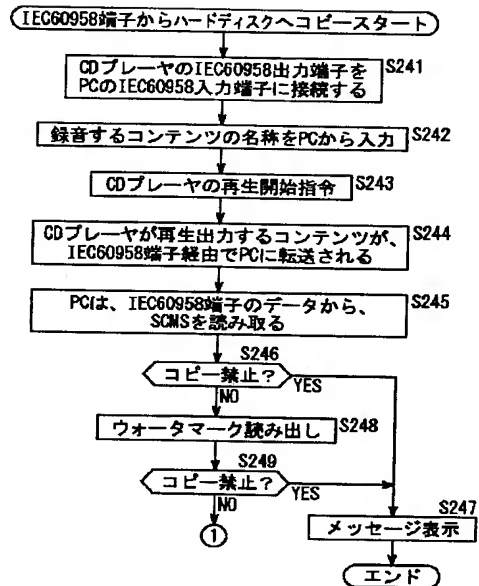
課金ログ

	アイテム1	アイテム2	アイテム3	
料金	50	50	60	
ハッシュ値	0xf8783e263517			

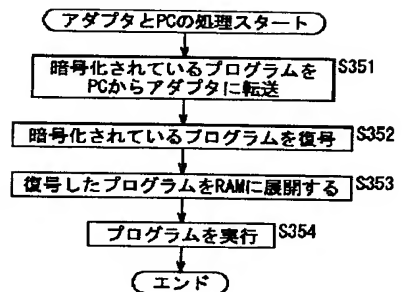
【図33】



【図26】

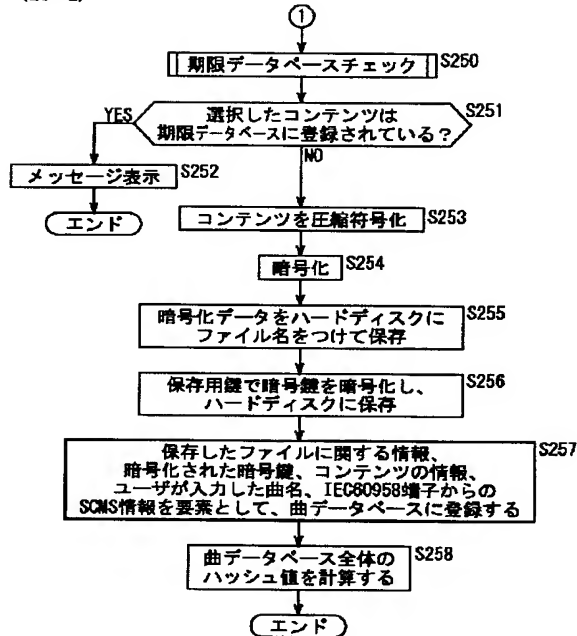


【図34】



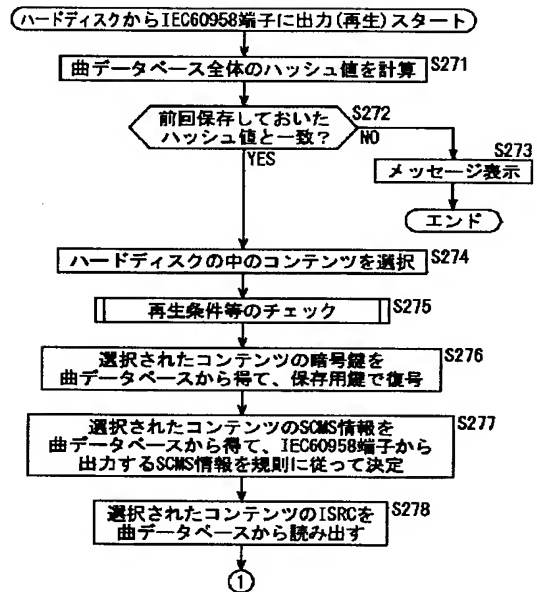
【図 27】

(26-2)



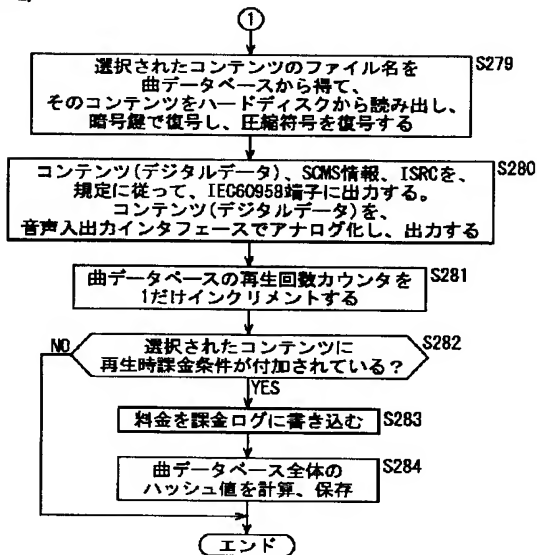
【図 28】

(28-1)

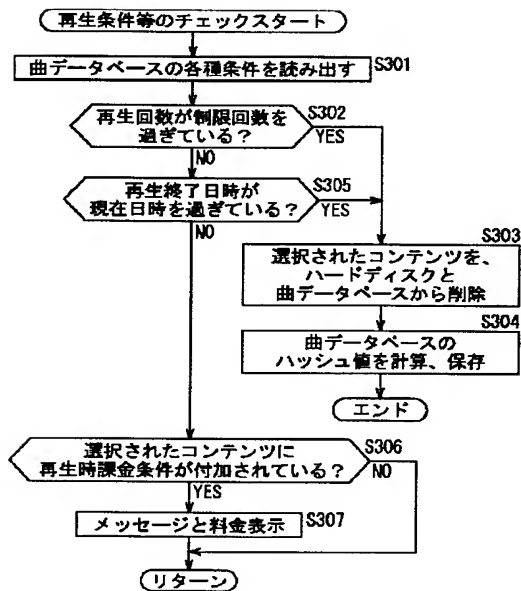


【図 29】

(28-2)

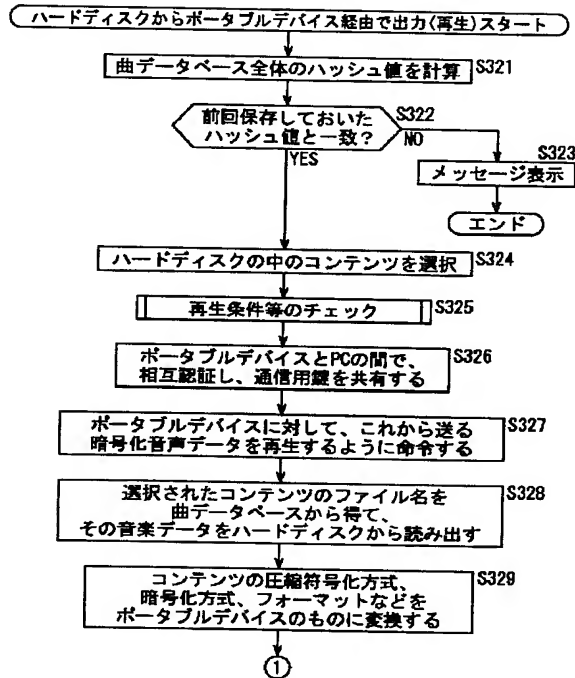


【図 30】



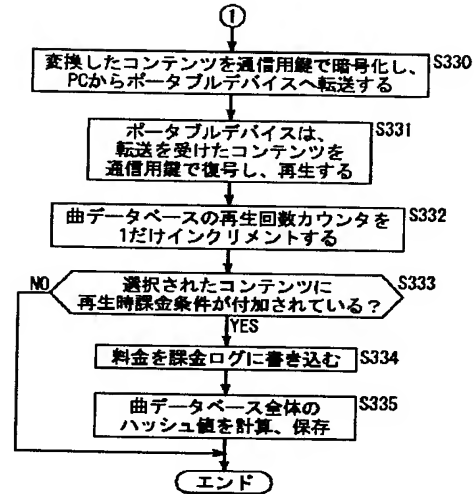
【図31】

(31-1)

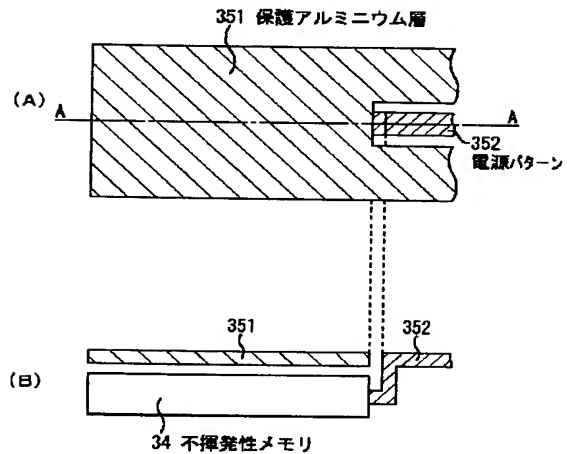


【図32】

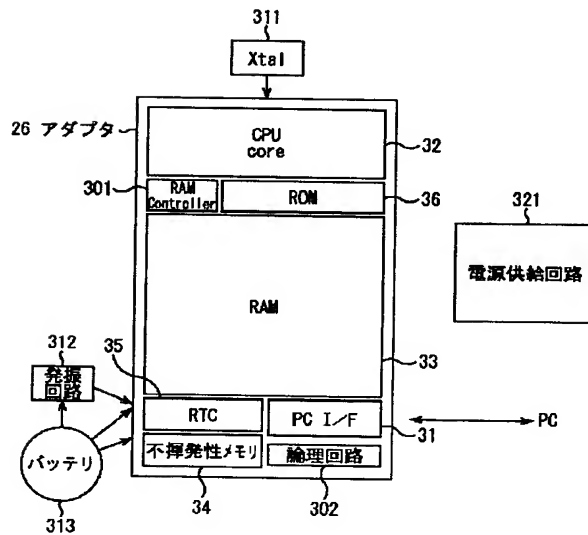
(31-2)



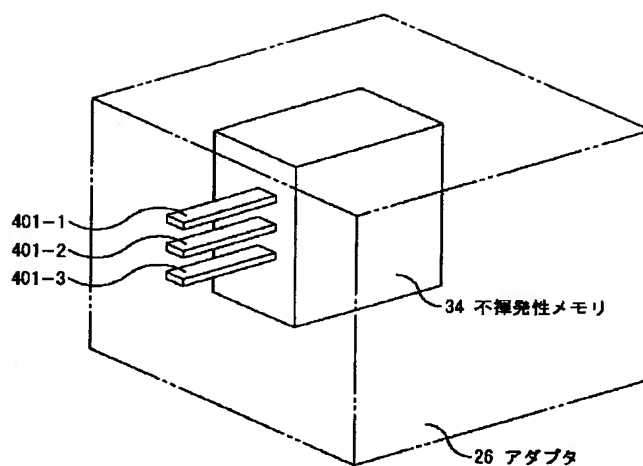
【図36】



【図35】



【図37】



フロントページの続き

(72)発明者 田辺 充
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 江面 裕一
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内